Purdue University

[Purdue e-Pubs](https://docs.lib.purdue.edu/)

[Department of Computer Science Technical](https://docs.lib.purdue.edu/cstech)

Department of Computer Science

2007

Enabling Confidentiality for Group Communication in Wireless Mesh Networks

Jing Dong

Cristina Nita-Rotaru Purdue University, crisn@cs.purdue.edu

Report Number: 07-010

Dong, Jing and Nita-Rotaru, Cristina, "Enabling Confidentiality for Group Communication in Wireless Mesh Networks" (2007). Department of Computer Science Technical Reports. Paper 1674. https://docs.lib.purdue.edu/cstech/1674

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

ENABLING CONFIDENTIALITY FOR GROUP ENABLING CONFIDENTIALITY FOR GROUP **COMUNNICATION IN WIRELESS MESH NETWORKS** COMUNNICATION IN WIRELESS MESH NETWORKS

Jing Dong Jing Dong **Cristina Nita-Rotaru** Cristina Nita-Rotaru

Department of Computer Science Department of Computer Science **Purdue University** Purdue University **West Lafayette, IN 47907** West Lafayette, IN 47907

> **CSD TR #07-010** CSD TR #07-010 **April 2007** April 2007

Enabling Confidentiality for Group Communication **Enabling Confidentiality for Group Communication** in Wireless Mesh Networks **in Wireless Mesh Networks**

Jing Dong Cristina Nita-Rotaru Jing Dong Cristina Nita-Rotaru Department of Computer Science, Purdue University Department of Computer Science, Purdue University 305 N. University St., West Lafayette, IN 47907 USA 305 N. University St., West Lafayette, IN 47907 USA {dongj,crisn) @cs.purdue.edu {dongj,crisn}@cs.purdue.edu

Abstract- **Wireless mesh networks (WMNs) have emerged as a** *Abstract-* Wireless mesh networks (WMNs) have emerged as a **promising technology for providing low-cost community wireless** promising technology for providing low-cost community wireless **services. Despite recent advancement in securing wireless net-**services. Despite recent advancement in securing wireless net**works, the problem of secure group communication on wireless** works, the problem of secure group communication on wireless **networks has received relatively little attention. Characteristics** networks has received relatively little attention. Characteristics **specific to WMNs, such as limited communication range and** specific to WMNs, such as limited communication range and **high link error rate, raise unique challenges in designing such** high link error rate, raise unique challenges in designing such **protocols.** protocols.

In this paper we focus on providing data confidentiality for In this paper we focus on providing data confidentiality for **group communications on WMNs. First, we propose W-LKH, a** group communications on WMNs. First, we propose W-LKH, a **protocol that combines centralized key management and reliable** protocol that combines centralized key management and reliable **key delivery, to address the less robust communication present** key delivery, to address the less robust communication present **in wireless networks. Next, we introduce WSOM, a new protocol** in wireless networks. Next, we introduce WSOM, a new protocol **framework designed specifically for the WMNs to overcome** framework designed specifically for the WMNs to overcome **the performance and security limitations of W-LKH. Simulation** the performance and security limitations of W-LKH. Simulation **results show that all of the proposed protocols can provide good** results show that all of the proposed protocols can provide good **performance to the upper layer applications, while the WSOM** performance to the upper layer applications, while the WSOM **protocols incur smaller overhead and are more responsive than** protocols incur smaller overhead and are more responsive than **W-LKH. Finally, we suggest the applicability of each of the** W-LKH. Finally, we suggest the applicability of each of the **proposed protocols under different application requirements.** proposed protocols under different application requirements.

I. INTRODUCTION 1. INTRODUCTION

Wireless mesh networks (WMNs) consist of a set of fixed Wireless mesh networks (WMNs) consist of a set of fixed wireless routers that form a multi-hop wireless backbone and wireless routers that form a multi-hop wireless backbone and a set of wireless clients. In recent years, WMNs have become a set of wireless clients. In recent years, WMNs have become a promising key technology for providing low-cost high-a promising key technology for providing low-cost highbandwidth community wireless services. Given the community bandwidth community wireless services. Given the community oriented nature of the WMNs, group applications such as real oriented nature of the WMNs, group applications such as real time conferencing, multimedia content broadcasting, and file time conferencing, multimedia content broadcasting, and file sharing are an important class of applications in the WMN sharing are an important class of applications in the WMN environment. As with other types of wireless applications, the environment. As with other types of wireless applications, the openness of the wireless environment makes security a critical openness of the wireless environment makes security a critical concern in deploying such group applications. concern in deploying such group applications.

The problem of securing group communication in traditional network environments has received significant attention, such network environments has received significant attention, such as the IP multicast [I], [2], [3] and overlay multicast networks as the IP multicast [1], [2], [3] and overlay multicast networks [4], [S], [6]. However, the constraints and peculiarities of the [4], [5], [6]. However, the constraints and peculiarities of the wireless medium are not considered by the protocols designed wireless medium are not considered by the protocols designed for wired networks, preventing them from being directly for wired networks, preventing them from being directly applied in the wireless environment. For example, the limited applied in the wireless environment. For example, the limited range of the wireless signal mandates multi-hop delivery of both unicast and multicast data, and hence precludes the both unicast and multicast data, and hence precludes the possibility of direct communication between nodes that some possibility of direct communication between nodes that some of the protocols for wired networks rely on. The limited communication range also necessitates the participation of non-munication range also necessitates the participation of group members in the data forwarding protocol which is absent group members in the data forwarding protocol which is absent in the wired networks. Furthermore, unreliable wireless links in the wired networks. Furthermore, unreliable wireless links

make loss recovery an essential component of the protocol, make loss recovery an essential component of the protocol, while scarce network bandwidth resource demands keeping while scarce network bandwidth resource demands keeping the overhead low to be a top priority in the protocol design. the overhead low to be a top priority in the protocol design.

The secure group communication problem and the related The secure group communication problem and the related key management problem have also been studied for wireless key management problem have also been studied for wireless sensor networks (WSNs) [7], [8], [91 and mobile ad hoc sensor networks (WSNs) [7], [8], [9] and mobile ad hoc networks (MANETs) [lo], [I 11, [12]. However, services for networks (MANETs) [10], [II], [12]. However, services for WSNs or MANETs were designed to sustain severe computa-WSNs or MANETs were designed to sustain severe tion power, storage, mobility and energy constraints, and as a tion power, storage, mobility and energy constraints, and as a result, they have limited scalability and robustness. As WMNs result, they have limited scalability and robustness. As WMNs have less restrictive constraints, they create opportunities for have less restrictive constraints, they create opportunities for designing more scalable and robust protocols. designing more scalable and robust protocols.

In this paper, we focus on the problem of ensuring data In this paper, we focus on the problem of ensuring data confidentiality for group communications on WMNs. We consider single-source group applications where a single source disseminates data to a dynamically changing set of receivers. disseminates data to a dynamically changing set of receivers. The main contributions of this paper are: The main contributions of this paper are:

- We study the design space for secure group communica-• We study the design space for secure group communication protocols on WMNs. We propose W-LKH, a central-tion protocols on WMNs. We propose W-LKH, a centralized membership protocol that combines the well-known ized membership protocol that combines the well-known protocol LKH [l] with reliable key delivery mechanisms, protocol LKH [1] with reliable key delivery mechanisms, and a new protocol framework WSOM with decentralized and a new protocol framework WSOM with decentralized membership management that overcomes the limitations membership management that overcomes the limitations inherent in W-LKH. inherent in W-LKH. . We compare all the proposed protocols analytically by • We compare all the proposed protocols analytically by
- examining the overhead and their responsiveness to the examining the overhead and their responsiveness to the upper layer applications. upper layer applications.
- We validate our design experimentally with extensive We validate our design experimentally with extensive simulations based on the *ns* simulator [13]. Simulation results show that all of the proposed protocols can provide results show that all of the proposed protocols can provide good performance to the upper layer applications, and good performance to the upper layer applications, and with proper optimization, the WSOM based protocols with proper optimization, the WSOM based protocols incur less overhead and are more responsive than W-incur less overhead and are more responsive than W-LKH. We also demonstrate that reliable key delivery is LKH. We also demonstrate that reliable key delivery is critical on WMNs. critical on WMNs.
- We discuss the applicability of each of the proposed We discuss the applicability of each of the proposed protocols under different application requirements. protocols under different application requirements.

The rest of the paper is organized as follows. We first The rest of the paper is organized as follows. We first present related work in Section 11. We then describe the present related work in Section II. We then describe the network and security model we consider in this work in network and security model we consider in this work in Section 111. We discuss the design goals and main challenges Section III. We discuss the design goals and main challenges in Section IV. Sections V and VI describe the W-LKH and the in Section IV. Sections V and VI describe the W-LKH and the WSOM protocols. We present the analytical and experimental WSOM protocols. We present the analytical and experimental comparison results for the proposed protocols in Section VII comparison results for the proposed protocols in Section VII and VIII, respectively. We conclude our paper in Section IX. and VIII, respectively. We conclude our paper in Section IX.

II. RELATED WORK

In this section, we review the existing work on the secure In this section, we review the existing work on the secure group communication problem for both wired networks and group communication problem for both wired networks and wireless networks. wireless networks.

The problem of secure group communication has received The problem of secure group communication has received significant attention for wired networks. In the context of the significant attention for wired networks. In the context of the IP multicast environment, the main focus was primarily to IP multicast environment, the main focus was primarily to reduce the computation overhead of key updates at the source. reduce the computation overhead of key updates at the source. The most well-known protocols are LKH [l] and its variants The most well-known protocols are LKH [1] and its variants [14], [IS], [16], 1171, [18]. The problem of key transportation [15], [16], [17], [18]. The problem of key transportation was studied both in the context of IP multicast [IS], [18] was studied both in the context of IP multicast [15], [18] and more recently in overlay networks [4], [19], [20], [21], and more recently in overlay networks [4], [19], [20], [21], [6]. In the latter case, overlays were used as a more realistic [6]. In the latter case, overlays were used as a more realistic structure to deliver keys due to lack of deployment of IP structure to deliver keys due to lack of deployment of IP multicast. However, none of these protocols considered the multicast. However, none of these protocols considered the wireless specific constraints and challenges, such as limited wireless specific constraints and challenges, such as limited bandwidth, multi-hop communication through possible non-bandwidth, multi-hop communication through possible nonmember nodes and higher link error rates. Thus these protocols member nodes and higher link error rates. Thus these protocols are not directly applicable to WMNs. are not directly applicable to WMNs.

In the wireless environment, work related to secure group In the wireless environment, work related to secure group communication focused on securing the multicast protocols communication focused on securing the multicast protocols and key management. The problem of securing the multicast and key management. The problem of securing the multicast protocol [22] is complementary to providing data confidential-protocol [22] is complementary to providing data ity, as it focuses only on the control message and not the data traffic. Several researchers [7], [8], [9] proposed schemes for traffic. Several researchers [7], [8], [9] proposed schemes for establishing pair-wise symmetric keys for sensor networks and establishing pair-wise symmetric keys for sensor networks and wireless ad hoc networks. These schemes focus on secure pair-wireless ad hoc networks. These schemes focus on secure pairwise communications instead of group communications. Zhu wise communications instead of group communications. Zhu et a1 [lo] proposed GKMPAN, a secure group communication et al [10] proposed GKMPAN, a secure group communication that uses symmetric keys to distribute the common group key that uses symmetric keys to distribute the common group key for data encryption among group members. The main focus of GKMPAN is on handling member revocations, instead of the GKMPAN is on handling member revocations, instead of the potentially much more frequent member join and leave events. potentially much more frequent member join and leave events. Moreover, GKMPAN requires key pre-distribution, which is Moreover, GKMPAN requires key pre-distribution, which is not always available, and a broadcast authentication scheme, not always available, and a broadcast authentication scheme, such as TESLA [23], which has the additional requirement of such as TESLA [23], which has the additional requirement of time synchronization. Balachandran et a1 proposed CRTDH time synchronization. Balachandran et al proposed CRTDH [ll] for secure group communication which relies on the [11] for secure group communication which relies on the Chinese Remainder Theorem and the Diffie-Hellman group Chinese Remainder Theorem and the Diffie-Hellman group key agreement for establishing group keys. The shortcoming key agreement for establishing group keys. The shortcoming of the CRTDH is that every group join and leave event requires of the CRTDH is that every group join and leave event requires the number of messages being delivered be proportional to the the number of messages being delivered be proportional to the group size, hence it is not scalable in a wireless environment group size, hence it is not scalable in a wireless environment where the bandwidth resource is scarce. Kaya et a1 [12] present where the bandwidth resource is scarce. Kaya et al [12] present a secure multicast scheme for mobile ad hoc networks. Instead, a secure multicast scheme for mobile ad hoc networks. Instead, our protocols focus on the WMNs which allow for further optimizations by exploiting the static network topology. optimizations by exploiting the static network topology.

111. NETWORK AND SECURITY MODEL III. NETWORK AND SECURITY MODEL

A. Network Model A. Network Model

Our target network environment is WMNs, where nodes Our target network environment is WMNs, where nodes are assumed to be static and communicate through multi-hop are assumed to be static and communicate through multi-hop wireless links. Possible link and node failures are allowed in wireless links. Possible link and node failures are allowed in the network. We focus on the group communication scenario the network. We focus on the group communication scenario where one data source broadcasts data to a set of receivers where one data source broadcasts data to a set of receivers (group members) that can dynamically change throughout (group members) that can dynamically change throughout the broadcast session. We assume a tree-based on-demand the broadcast session. We assume a tree-based on-demand multicast protocol is used to deliver the group data. For con-multicast protocol is used to deliver the group data. For concreteness, we consider the well-known MAODV [24] protocol creteness, we consider the well-known MAODV [24] protocol in presenting our protocols. in presenting our protocols.

Due to the multi-hop communication of WMNs, it is neces-Due to the multi-hop communication of WMNs, it is necessary that non-group members participate in the multicast tree sary that non-group members participate in the multicast tree construction. Hence, the multicast tree contains two types of construction. Hence, the multicast tree contains two types of nodes: *member nodes* and *nonmember nodes.* Member nodes nodes: *member nodes* and *non-member nodes.* Member nodes are nodes on the tree that are also members of the multicast are nodes on the tree that are also members of the multicast group. The non-member nodes are not part of the multicast group. The non-member nodes are not part of the multicast group but rather act as routers that help to connect the member group but rather act as routers that help to connect the member nodes. We refer to the nodes in the multicast tree (both member nodes. We refer to the nodes in the multicast tree (both member and non-member) as *tree nodes.* Nodes that are not part of the and non-member) as *tree nodes.* Nodes that are not part of the multicast tree are called *non-tree* nodes. multicast tree are called *non-tree* nodes.

B. Security and Adversarial Model B. Security and Adversarial Model

Our focus is on providing confidentiality of the data from Our focus is on providing confidentiality of the data from outside adversaries, where an outsider is any non-member node, including non-member nodes that are on the multicast node, including non-member nodes that are on the multicast tree. Nodes that have left the group are also considered tree. Nodes that have left the group are also considered outsiders. We assume that the current group members do not leak data or keys to non-authorized nodes. leak data or keys to non-authorized nodes.

We assume there is a group manager that manages that We assume there is a group manager that manages that group membership. The group manager acts as a certificate group membership. The group manager acts as a certificate authority (CA) for the group, responsible for issuing member authority (CA) for the group, responsible for issuing member certificates that bind a member's public key to the group IP certificates that bind a member's public key to the group IP address and for revoking group memberships. We also assume address and for revoking group memberships. We also assume all group members know the public key of the group manager, all group members know the public key of the group manager, so that all member certificates can be verified by any group so that all member certificates can be verified by any group member. member.

We do not consider attacks against the multicast protocol We do not consider attacks against the multicast protocol itself. For example, we do not consider denial of service (DoS) attacks against data forwarding and assume both group (DoS) attacks against data forwarding and assume both group members and non-member nodes forward application and members and non-member nodes forward application and control data according to the protocol specification. Protecting control data according to the protocol specification. Protecting the multicast protocol is complementary to our work. the multicast protocol is complementary to our work.

IV. DESIGN SPACE IV. DESIGN SPACE

The security goal of our protocol is to ensure data confiden-The security goal of our protocol is to ensure data confidentiality. However, this goal should not be achieved at the price tiality. However, this goal should not be achieved at the price of sacrificing performance and robustness. More specifically, of sacrificing performance and robustness. More specifically, properties we want to achieve are: properties we want to achieve are:

Group secrecy: this property makes it computationally • Group secrecy: this property makes it computationally infeasible for a non-member node to discover the group data; infeasible for a non-member node to discover the group data; this also includes properties like forward or backward secrecy this also includes properties like forward or backward secrecy which guarantee that it is computationally infeasible for a which guarantee that it is computationally infeasible for a member node to get access to group data before joining the member node to get access to group data before joining the group, or after leaving (or being revoked from) the group, group, or after leaving (or being revoked from) the group, respectively. respectively.

Efficiency: the wireless environment requires that the pro-• Efficiency: the wireless environment requires that the tocol be efficient in terms of both communication cost and tocol be efficient in terms of both communication cost and computation cost. computation cost.

Robustness: the protocol should be resilient to unreliable • Robustness: the protocol should be resilient to unreliable links and possible link and node failures. links and possible link and node failures.

Performance: the secure protocol should maintain similar • Performance: the secure protocol should maintain similar data throughput to the upper layer application as the unsecured data throughput to the upper layer application as the unsecured protocol. protocol.

Efficient confidentiality and integrity of data delivery for Efficient confidentiality and integrity of data delivery for group communication can be achieved by using symmetric-group communication can be achieved by using symmetrickey based cryptographic algorithms. We consider two main key based cryptographic algorithms. We consider two main approaches: one relies on using a common key to encrypt and approaches: one relies on using a common key to encrypt and decrypt the data, while the other uses per-hop keys to achieve decrypt the data, while the other uses per-hop keys to achieve the same goals. the same goals.

Common-key based approach. In this approach, the critical Common-key based approach. In this approach, the critical component is the protocol that defines how the common data component is the protocol that defines how the common data encrypting key (also referred as *group key)* is computed and encrypting key (also referred as *group key)* is computed and disseminated. Such protocols are also referred to as *group key* disseminated. Such protocols are also referred to as *group key management protocols.* Although the group key management *management protocols.* Although the group key management protocols are already extensively studied for the wired net-protocols are already extensively studied for the wired networks, the unique characteristics of wireless communication works, the unique characteristics of wireless communication introduces new challenges that require new solutions tailored introduces new challenges that require new solutions tailored for the wireless environment. For example, many previously for the wireless environment. For example, many previously proposed protocols were designed under the assumption that proposed protocols were designed under the assumption that there exist mechanisms for reliable key delivery. However, there exist mechanisms for reliable key delivery. However, in the wireless environment, links are inherently much less in the wireless environment, links are inherently much less reliable. In addition, the multi-hop nature of wireless com-reliable. In addition, the multi-hop nature of wireless munication exacerbates the problem of unreliable links, since munication exacerbates the problem of unreliable links, since missing one key packet at one node affects all downstream missing one key packet at one node affects all downstream nodes that rely on this node. Therefore,' achieving efficient nodes that rely on this node. Therefore; achieving efficient reliable key delivery is a critical component for group key reliable key delivery is a critical component for group key management protocols in wireless networks. Compared to management protocols in wireless networks. Compared to the wired networks, the key delivery structure is also less the wired networks, the key delivery structure is also less straightforward in the wireless environment. On one hand, the straightforward in the wireless environment. On one hand, the existing group data delivery structure may not be optimized existing group data delivery structure may not be optimized for delivering keys, since keys have much more stringent for delivering keys, since keys have much more stringent reliability requirement than data. On the other hand, building a customized delivery structure for keys requires additional a customized delivery structure for keys requires additional protocols for handling of possible link and node failures. protocols for handling of possible link and node failures. Careful selection of the key delivery structure is necessary Careful selection of the key delivery structure is necessary for wireless networks. for wireless networks.

Per-hop key based approach. In the per-hop key based approach, the group data is encrypted hop-by-hop by relying on proach, the group data is encrypted hop-by-hop by relying on the secure channels established between group members. One the secure channels established between group members. One of the main challenges for such protocols in the wireless environment is that group members do not directly communicate with each other. Therefore, non-member nodes are required with each other. Therefore, non-member nodes are required in the establishment of the secure channels, which introduces in the establishment of the secure channels, which introduces additional security concerns. Secondly, the straightforward additional security concerns. Secondly, the straightforward way of using hop-by-hop encryption disallows the use of way of using hop-by-hop encryption disallows the use of broadcast for data dissemination, instead hop-by-hop unicast broadcast for data dissemination, instead hop-by-hop unicast must be used. Additional mechanisms are required for the per-must be used. Additional mechanisms are required for the perhop key approach to take advantage of the broadcast nature hop key approach to take advantage of the broadcast nature of wireless communication for data dissemination. of wireless communication for data dissemination.

Given the above described design space and challenges, in Given the above described design space and challenges, in the rest of the paper, we first present a protocol that adopts the the rest of the paper, we first present a protocol that adopts the common key based approach and several other protocols that common key based approach and several other protocols that adopt the per-hop key based approach. We will discuss in detail adopt the per-hop key based approach. We will discuss in detail how these protocols address the challenges in the wireless how these protocols address the challenges in the wireless

networks, and describe their advantages and limitations. networks, and describe their advantages and limitations.

V. A CENTRALIZED KEY MANAGEMENT PROTOCOL

In this section, we present W-LKH, a secure group commu-In this section, we present W-LKH, a secure group communication for WMNs that uses the common key based approach. nication for WMNs that uses the common key based approach. We first provide an overview of W-LKH, then describe its We first provide an overview of W-LKH, then describe its reliable key delivery mechanisms, and finally discuss its lim-reliable key delivery mechanisms, and finally discuss its limitations. itations.

A. Overview of W-LKH A. *Overview of W-LKH*

W-LKH is based on a well-known centralized scheme, LKH. W-LKH is based on a well-known centralized scheme, LKH. We selected LKH because it was intensively studied and it was We selected LKH because it was intensively studied and it was shown to work well in wired networks. We chose its batching shown to work well in wired networks. We chose its batching variant [14], which we refer to as B-LKH, given the benefits variant [14], which we refer to as B-LKH, given the benefits of batching in reducing the computation and communication of batching in reducing the computation and communication overhead. overhead.

In W-LKH, data is encrypted using a group key and In W-LKH, data is encrypted using a group key and delivered on the multicast tree. In order to ensure forward delivered on the multicast tree. In order to ensure forward and backward secrecy of the group data, at every join and and backward secrecy of the group data, at every join and leave event, the source is notified and a new key is generated leave event, the source is notified and a new key is generated and distributed to the current group members. As in B-LKH, and distributed to the current group members. As in B-LKH, the source maintains a logical key tree to ensure a logarithmic the source maintains a logical key tree to ensure a logarithmic bound for the size of the message rekey. The main difference bound for the size of the message rekey. The main difference between W-LKH and B-LKH is the message delivery process. between W-LKH and B-LKH is the message delivery process.

Delivery of join and leave messages: In order to maintain *Delivery of join and leave messages:* In order to maintain the consistency of the logical key tree maintained at the source, the join and leave requests have to be delivered via reliable the join and leave requests have to be delivered via reliable channels. The TCP protocol, which is normally used in wired channels. The TCP protocol, which is normally used in wired networks, does not work well for the delivery of the join networks, does not work well for the delivery of the join and leave requests on WMNs, as building a TCP session and leave requests on WMNs, as building a TCP session requires several round trip time and the delivery of several control packets, and consequently results in large latency control packets, and consequently results in large latency and bandwidth overhead. Instead, we use a simple reliable and bandwidth overhead. Instead, we use a simple reliable transport protocol which involves only an ACK from the transport protocol which involves only an ACK from the receiver to ensure reliable delivery. Therefore, for most cases, receiver to ensure reliable delivery. Therefore, for most cases, only one round trip time and one additional control message are required to complete a join or leave request. are required to complete a join or leave request.

B. Rekey Message Transportation B. Rekey Message Transportation

The responsibility of the rekey message transportation pro-The responsibility of the rekey message transportation process is to deliver the rekey messages generated by the data cess is to deliver the rekey messages generated by the data source reliably to each group member. The approach we use source reliably to each group member. The approach we use for the rekey message transportation is to enhance the existing for the rekey message transportation is to enhance the existing MAODV tree built for the data delivery with hop-by-hop MAODV tree built for the data delivery with hop-by-hop reliability for delivering the rekey messages, such that each node retransmits the rekey message until all of its downstream node retransmits the rekey message until all of its downstream members receives the message. members receives the message.

I) *Hop-by-Hop Reliable Key Delivery:* The most common *1) Hop-by-Hop Reliable Key Delivery:* The most common approach to the hop-by-hop reliable delivery is the ACK approach to the hop-by-hop reliable delivery is the ACK mechanism, where the receiver sends an ACK to the sender mechanism, where the receiver sends an ACK to the sender after receiving a message, as in the 802.1 1 unicast protocol. after receiving a message, as in the 802.11 unicast protocol. However, since in the multicast environment, there are usually However, since in the multicast environment, there are usually multiple downstream receivers for each rekey message, the multiple downstream receivers for each rekey message, the ACK mechanism can cause the well-known ACK implosion ACK mechanism can cause the well-known ACK implosion problem. Instead, we choose to use the NACK mechanism, problem. Instead, we choose to use the NACK mechanism, where a node sends a NACK to the sender when it detects where a node sends a NACK to the sender when it detects

packet misses. The missing of rekey messages can be detected packet misses. The missing of rekey messages can be detected when a node receives a data packet encrypted with an unknown when a node receives a data packet encrypted with an unknown key. Since receiving data packets is a frequent event, the key. Since receiving data packets is a frequent event, the detection of missing keys happens quickly. Compared to the detection of missing keys happens quickly. Compared to the ACK mechanism, the NACK mechanism also has the benefit ACK mechanism, the NACK mechanism also has the benefit of smaller overhead, as it is expected that the probability of a node receiving a rekey message is greater than the probability node receiving a rekey message is greater than the probability of missing the message. of missing the message.

To further reduce the protocol overhead, we exploit the To further reduce the protocol overhead, we exploit the broadcast nature of wireless signal by applying the NACK broadcast nature of wireless signal by applying the NACK suppression technique [25]. With the NACK suppression technique, when a node detects that it misses a rekey message, nique, when a node detects that it misses a rekey message, instead of firing the NACK immediately, it sets a NACK instead of firing the NACK immediately, it sets a NACK timer with a random timeout up to some maximum value. timer with a random timeout up to some maximum value. If it receives a NACK from another node requesting the same If it receives a NACK from another node requesting the same rekey message before its NACK timer expires, it resets its rekey message before its NACK timer expires, it resets its NACK timeout value. The NACK timer is cancelled once NACK timeout value. The NACK timer is cancelled once the node receives the missing rekey message it requested. the node receives the missing rekey message it requested. Since most downstream nodes are close to each other, for Since most downstream nodes are close to each other, for most cases only one NACK message is necessary even though most cases only one NACK message is necessary even though multiple downstream nodes miss the same rekey message. multiple downstream nodes miss the same rekey message. Furthermore, if the NACK timer is set small enough, the Furthermore, if the NACK timer is set small enough, the missing rekey message can be recovered before the next data missing rekey message can be recovered before the next data packet is broadcasted by the parent. This allows for time packet is broadcasted by the parent. This allows for time sensitive applications to resume the decryption of data as soon sensitive applications to resume the decryption of data as soon as possible while keeping the overhead low. as possible while keeping the overhead low.

2) *Rekey Message Recovery:* Even with hop-by-hop relia-*2) Rekey Message Recovery:* Even with hop-by-hop bility, a number of rekey messages can still be lost for a large bility, a number of rekey messages can still be lost for a large duration of time for a particular node due to link or node duration of time for a particular node due to link or node failures and network partitions. In such cases, the key recovery failures and network partitions. In such cases, the key recovery procedure is invoked to recover the missing keys. Instead of procedure is invoked to recover the missing keys. Instead of requesting the missing packets directly from the data source, as requesting the missing packets directly from the data source, as in the wired network, we adopt a local recovery procedure in in the wired network, we adopt a local recovery procedure in order to minimize the bandwidth overhead while not affecting the application performance. the application performance.

The local recovery procedure is only invoked at a node The local recovery procedure is only invoked at a node when the node can receive a continuous stream of data packets when the node can receive a continuous stream of data packets from its upstream node, as the continuous stream of data packets indicates the path between the node and the data packets indicates the path between the node and the data source is functional. To initiate the local recovery process, the source is functional. To initiate the local recovery process, the node transmits a NACK packet containing all the sequence node transmits a NACK packet containing all the sequence numbers of the missing rekey messages to its tree parent. numbers of the missing rekey messages to its tree parent. Once the tree parent receives the NACK packet, it sends to Once the tree parent receives the NACK packet, it sends to the requesting node the requested rekey messages for which the requesting node the requested rekey messages for which it has already received. For the other rekey messages, a local it has already received. For the other rekey messages, a local recovery procedure is recursively invoked on the tree parent. The process repeats until all the requested rekey messages are The process repeats until all the requested rekey messages are delivered to the original requesting node. delivered to the original requesting node.

Note that in the above described local recovery process, Note that in the above described local recovery process, it is necessary for each node to buffer the rekey messages it is necessary for each node to buffer the rekey messages that it receives for some period of time so that the request for missing rekey messages from downstream nodes can be for missing rekey messages from downstream nodes can be satisfied as locally as possible. Since rekey messages are of small size and are issued infrequently with the batch rekeying small size and are issued infrequently with the batch rekeying technique, it is feasible for each nodes to buffer recent rekey technique, it is feasible for each nodes to buffer recent rekey messages for the purpose of rekey message recovery. messages for the purpose of rekey message recovery.

3) Data and Key Message Ordering: Since in the above *3) Data and Key Message Ordering:* Since in the above rekey transportation and recovery scheme the missing of rekey messages is detected by receiving data packets that are encrypted with unknown keys, we require that each node are encrypted with unknown keys, we require that each node forwards only data packets for which it has the decryption key forwards only data packets for which it has the decryption key and buffers undecryptable data packets until the corresponding and buffers undecryptable data packets until the corresponding decryption key has been received and forwarded to the down-decryption key has been received and forwarded to the downstream node. This requirement minimizes the out-of-order stream node. This requirement minimizes the out-of-order problem of key and data message, thus reducing the number problem of key and data message, thus reducing the number of NACKs for missing key messages. Under most cases, it also ensures that when a node receives a NACK for a rekey also ensures that when a node receives a NACK for a rekey message, it has already received the requested rekey message, message, it has already received the requested rekey message, thus recursive propagation of NACK message is eliminated. thus recursive propagation of NACK message is eliminated. Note that delaying forwarding undecryptable packets does not Note that delaying forwarding undecryptable packets does not affect the data throughput for the application, as a packet affect the data throughput for the application, as a packet undecryptable in a node is necessarily undecryptable in its downstream nodes. downstream nodes.

C. Limitations of W-LKH C. *Limitations of W-LKH*

Although W-LKH has been optimized for the WMNs, it Although W-LKH has been optimized for the WMNs, it still has several limitations. First, the join and leave requests still has several limitations. First, the join and leave requests require message exchanges between the joining or leaving node to the data source. Depending on the distance from the node to the data source. Depending on the distance from the joining or leaving node to the data source, this operation can joining or leaving node to the data source, this operation can incur significant latency and bandwidth overhead. Second, the incur significant latency and bandwidth overhead. Second, the rekey message which includes key encryptions required by rekey message which includes key encryptions required by all the group members needs to be transmitted throughout all the group members needs to be transmitted throughout the multicast tree, even though typically only a subset of the multicast tree, even though typically only a subset of the encryptions are required by a particular branch of the the encryptions are required by a particular branch of the tree. Finally, the use of batching for reducing the bandwidth tree. Finally, the use of batching for reducing the bandwidth overhead also causes partial loss of the forward and backward overhead also causes partial loss of the forward and backward data secrecy. These limitations are the consequence of the fun-data secrecy. These limitations are the consequence of the fundamental design choice made by the LKH scheme, centralized damental design choice made by the LKH scheme, centralized group membership management, where the data source is the group membership management, where the data source is the central point that handles all group join and leave events. central point that handles all group join and leave events.

VI. SECURE OVERLAY BASED SECURE MULTICAST IN VI. SECURE OVERLAY BASED SECURE MULTICAST IN WMNs WMNs

In this section, we present a new secure multicast protocol In this section, we present a new secure multicast protocol framework, WSOM, that uses the decentralized membership framework, WSOM, that uses the decentralized membership management principle to address the limitations in W-LKH. management principle to address the limitations in W-LKH. We first provide an overview of the framework, then present We first provide an overview of the framework, then present three different protocols and a member revocation mechanism. three different protocols and a member revocation mechanism.

A. Overview of WSOM A. *Overview of WSOM*

The WSOM framework is based on an overlay tree main-The WSOM framework is based on an overlay tree maintained on top of the data delivery multicast tree. The overlay tained on top of the data delivery multicast tree. The overlay consists of only member nodes and two member nodes are consists of only member nodes and two member nodes are connected on the overlay if they are adjacent in the underlying connected on the overlay if they are adjacent in the underlying multicast tree disregarding non-member nodes. Figure 1 shows multicast tree disregarding non-member nodes. Figure I shows an example of the overlay structure for a sample multicast sce-an example of the overlay structure for a sample multicast scenario. Neighboring nodes on the overlay maintain a symmetric nario. Neighboring nodes on the overlay maintain a symmetric key, referred to as *link key,* between them, which establishes key, referred to as *link key,* between them, which establishes a secure channel between these two nodes. We refer to this a secure channel between these two nodes. We refer to this overlay network as a *secure overlay*. Since we only consider tree based multicast structure, the overlay structure we just tree based multicast structure, the overlay structure we just

described is necessarily a tree. For convenience, we use the term overlay parent, overlay children and overlay neighbor to refer to the parent, children, and neighbor of a node in the overlay, respectively.

Maintenance of the Secure Overlay: The key for maintain-*Maintenance of the Secure Overlay:* The key for maintaining the secure overlay is for each node to maintain an updated ing the secure overlay is for each node to maintain an updated link key with its overlay neighbors as the underlying multicast link key with its overlay neighbors as the underlying multicast tree changes, which can be caused by group join, group leave, tree changes, which can be caused by group join, group leave, and link and node failures. We now present the operations and link and node failures. We now present the operations required for handling each such event in detail. required for handling each such event in detail.

For group joins, after being part of the multicast tree, the For group joins, after being part of the multicast tree, the joining node communicates with its overlay parent along the joining node communicates with its overlay parent along the multicast tree path to establish a link key using the standard multicast tree path to establish a link key using the standard public key infrastructure *(PKI)* techniques. If the joining node public key infrastructure *(PKl)* techniques. If the joining node is already a tree node before joining, it also needs to build a is already a tree node before joining, it also needs to build a link key with each of its overlay children. To accomplish this, link key with each of its overlay children. To accomplish this, the joining node broadcasts a parent change packet including the joining node broadcasts a parent change packet including its member certificate downward along the tree. Each of its its member certificate downward along the tree. Each of its overlay children, upon receiving the parent change packet, generates a random link key and sends it to the joining node generates a random link key and sends it to the joining node after proper signing and encrypting using the standard *PKI* after proper signing and encrypting using the standard PKI techniques. For graceful group leaves, the overlay parent of techniques. For graceful group leaves, the overlay parent of the leaving node is notified of the event and establishes link the leaving node is notified of the event and establishes link keys with the overlay children of the leaving node in a way keys with the overlay children of the leaving node in a way that is similar to when the joining node builds link keys with that is similar to when the joining node builds link keys with its overlay children. For ungraceful leaves and link and node its overlay children. For ungraceful leaves and link and node failures, the link keys are re-established once the downstream failures, the link keys are re-established once the downstream nodes get reconnected back to the tree much like the joining nodes get reconnected back to the tree much like the joining case. case.

Note that in handling all of the above events, only local Note that in handling all of the above events, only local message exchanges are required. Moreover, in the WMN message exchanges are required. Moreover, in the WMN environment, where all nodes are static, most changes on the underlying multicast tree are due to group join and leave the underlying multicast tree are due to group join and leave events. Therefore, for stable groups and network environment, events. Therefore, for stable groups and network environment, the overhead for maintaining the secure overlay is very small. the overhead for maintaining the secure overlay is very small.

B. WSOM Protocols B. WSOM Protocols

In this section, we present three different secure multicast In this section, we present three different secure multicast protocols that use the secure overlay structure as described in protocols that use the secure overlay structure as described in the previous section: WSOM-GK, WSOM-LK, and WSOM-HK. HK.

I) WSOM-GK: WSOM with Group Key for Data Encryp-1) WSOM-GK: WSOM with Group Key for Data Encryption: In this protocol, a group key is maintained among all *tion:* In this protocol, a group key is maintained among all group members. The group data is encrypted with the group group members. The group data is encrypted with the group key at the source, then disseminated on the multicast tree. key at the source, then disseminated on the multicast tree. The source periodically refreshes the group key by generating The source periodically refreshes the group key by generating a new group key. The new group key is disseminated to all a new group key. The new group key is disseminated to all group members using the secure overlay. group members using the secure overlay.

For group joins, besides updating the secure overlay, the For group joins, besides updating the secure overlay, the overlay parent of the joining node piggy-backs the current overlay parent of the joining node piggy-backs the current group key on the messages required for updating the secure group key on the messages required for updating the secure overlay, so that the joining node can start decrypting group overlay, so that the joining node can start decrypting group data immediately. For group leaves, only the update of the data immediately. For group leaves, only the update of the secure overlay is required. Key loss due to node or link failures secure overlay is required. Key loss due to node or link failures can be handled in a way similar to the local key recovery can be handled in a way similar to the local key recovery strategy in W-LKH. strategy in W-LKH.

The main limitation of this protocol is that it suffers The main limitation of this protocol is that it suffers from partial loss of the forward and backward data secrecy. from partial loss of the forward and backward data secrecy. However, the application can adjust the key refreshment period However, the application can adjust the key refreshment period to balance the bandwidth overhead and the loss of the forward to balance the bandwidth overhead and the loss of the forward and backward secrecy. and backward secrecy.

2) *WSOM-LK: WSOM with Link Key for Data Encryption: 2) WSOM-LK: WSOM with Link Key for Data Encryption:* In this protocol, the group data is delivered directly on the In this protocol, the group data is delivered directly on the secure overlay. To forward a data packet, the node encrypts secure overlay. To forward a data packet, the node encrypts the data packet with the link key of each of its overlay children the data packet with the link key of each of its overlay children and then forwards the encrypted packet to the corresponding and then forwards the encrypted packet to the corresponding children. This basic scheme suffers from two drawbacks. First, children. This basic scheme suffers from two drawbacks. First, re-encrypting the data packet for each of the overlay children re-encrypting the data packet for each of the overlay children requires computation cost linear to the number of overlay requires computation cost linear to the number of overlay children for each node, which can be significant for nodes with children for each node, which can be significant for nodes with many children. Second, it is impossible to exploit the broadcast many children. Second, it is impossible to exploit the broadcast nature of wireless transmission, as each of the encrypted data nature of wireless transmission, as each of the encrypted data packet is only useful for one downstream child. To overcome packet is only useful for one downstream child. To overcome these drawbacks, instead of using link keys to encrypt the data these drawbacks, instead of using link keys to encrypt the data packets directly, the source encrypts the data packet with a randomly generated data encryption key (k_d) . To disseminate the data packet, the source encrypts k_d with the link key of each of its overlay children, piggy-backs all the encryptions each of its overlay children, piggy-backs all the encryptions of k_d to the data packet, and then broadcasts the packet on the multicast tree. When a member node receives an encrypted the multicast tree. When a member node receives an encrypted packet, it can decrypt the packet by first decrypting k_d with its corresponding link key and then using k_d to decrypt the data packet. For forwarding the received packet to its downstream packet. For forwarding the received packet to its downstream nodes, the member node re-encrypts k_d with the link keys of its overlay children, and replaces the k_d encryptions on the received packet with the new set of encryptions of k_d . Although the number of encryptions required for each node is Although the number of encryptions required for each node is also linear to the number of overlay children of the node, this also linear to the number of overlay children of the node, this scheme is still computation-wise efficient, as the size of k_d is typically only 128 bits. typically only 128 bits.

Since no additional control data is maintained in WSOM-Since no additional control data is maintained in WSOM-LK, the handling of join and leave events only requires LK, the handling of join and leave events only requires updating the secure overlay. Unlike WSOM-GK, this protocol updating the secure overlay. Unlike WSOM-GK, this protocol does not suffer from key loss problem. does not suffer from key loss problem.

3) *WSOM-HK: WSOM with Hop Key for Data Encryption: 3) WSOM-HK: WSOM with Hop Key for Data Encryption:* In WSOM-LK, even with the optimization of using data In WSOM-LK, even with the optimization of using data encryption keys, there is still per data packet computation and encryption keys, there is still per data packet computation and

bandwidth overhead on each member node for encrypting and bandwidth overhead on each member node for encrypting and delivering the key for each of its overlay children. The aim of delivering the key for each of its overlay children. The aim of WSOM-HK is to reduce both the computation and bandwidth WSOM-HK is to reduce both the computation and bandwidth overhead by maintaining a hop key among every member node overhead by maintaining a hop key among every member node and its overlay children. With the help of the hop key, the data and its overlay children. With the help of the hop key, the data encryption key only needs to be encrypted once with the hop encryption key only needs to be encrypted once with the hop key and only one encryption of the key needs to be appended key and only one encryption of the key needs to be appended to the data packet for forwarding to the downstream nodes, to the data packet for forwarding to the downstream nodes, instead of one for each overlay child as in the WSOM-LK instead of one for each overlay child as in the WSOM-LK protocol. protocol.

Each hop key can be regarded as a mini group key with Each hop key can be regarded as a mini group key with the member node as the source and its overlay children as the member node as the source and its overlay children as the group members. Due to the small scale, a straightforward the group members. Due to the small scale, a straightforward approach, such as encrypting and delivering the new hop key approach, such as encrypting and delivering the new hop key to each of the overlay children whenever the overlay children to each of the overlay children whenever the overlay children set changes, can be employed to maintain the hop key. set changes, can be employed to maintain the hop key.

The cost of maintaining a hop key is amortized over all The cost of maintaining a hop key is amortized over all the data packets delivered using that key. Unlike WSOM-LK the data packets delivered using that key. Unlike WSOM-LK scheme, this scheme has lower per packet overhead. scheme, this scheme has lower per packet overhead.

C. Revocation in the WSOM Based Protocols C. *Revocation in the WSOM Based Protocols*

Unlike in the centralized membership management schemes Unlike in the centralized membership management schemes where member revocations can be easily performed by the cen-where member revocations can be easily performed by the central point, in decentralized membership management schemes, tral point, in decentralized membership management schemes, a separate membership revocation mechanism has to be pro-a separate membership revocation mechanism has to be provided. Instead of using the straightforward certificate re-vided. Instead of using the straightforward certificate revocation list (CRL) approach, which requires the reliable vocation list (CRL) approach, which requires the reliable delivery of the CRLs to all group members, we design a delivery of the CRLs to all group members, we design a new more efficient revocation mechanisms for the WSOM new more efficient revocation mechanisms for the WSOM based protocols. The main observation we exploit is that based protocols. The main observation we exploit is that under the static topology of WMNs, it is possible to restrict under the static topology of WMNs, it is possible to restrict a node to join the secure overlay only through a few nearby a node to join the secure overlay only through a few nearby member nodes, which we will refer to as the *join points* of member nodes, which we will refer to as the *join points* of the node. Then to revoke a member node, it is sufficient to the node. Then to revoke a member node, it is sufficient to delivery the revocation notice to only the small number of delivery the revocation notice to only the small number of join points of the node, instead of to the whole group, thus join points of the node, instead of to the whole group, thus saving the network bandwidth. In the following, we describe saving the network bandwidth. In the following, we describe the details of the revocation protocol together with the required the details of the revocation protocol together with the required changes on the WSOM protocol. For convenience, we refer to our revocation protocol as *WSOM-revoke* and the entity to our revocation protocol as *WSOM-revoke* and the entity responsible for issuing and revoking the member certificates responsible for issuing and revoking the member certificates as the group manager. as the group manager.

1) *Overview of WSOM-revoke:* With WSOM-revoke, prior *1) Overview of WSOM-revoke:* With WSOM-revoke, prior to obtaining the member certificate, the node attempting to to obtaining the member certificate, the node attempting to join the group selects a set of its nearby member nodes as join the group selects a set of its nearby member nodes as its join points. Then during the process obtaining the member its join points. Then during the process obtaining the member certificate, the node provides the pre-selected join points to certificate, the node provides the pre-selected join points to the group manager, which then saves the join points and also the group manager, which then saves the join points and also includes them in the member certificate for the node. To join includes them in the member certificate for the node. To join the secure overlay, the node only activates the multicast tree the secure overlay, the node only activates the multicast tree branch that leads to one of its pre-selected join points, which branch that leads to one of its pre-selected join points, which we will refer to its *actual join point.* The actual join point we will refer to its *actual join point.* The actual join point verifies that itself is in the set of pre-selected join points of verifies that itself is in the set of pre-selected join points of the joining node by checking the node's member certificate and the joining node by checking the node's member certificate and that the joining node is not revoked before admitting the node that the joining node is not revoked before admitting the node as its overlay child. Now, to revoke a member node, the group as its overlay child. Now, to revoke a member node, the group manager only needs to delivery the revocation notice to the manager only needs to delivery the revocation notice to the pre-selected join points of the node¹. Once all the join points of the node receive the revocation notice, the node can no of the node receive the revocation notice, the node can no longer join the secure overlay, thus loses its ability to decrypt longer join the secure overlay, thus loses its ability to decrypt the group data. the group data.

2) Details of WSOM-revoke: Now we discuss some more *2) Details of WSOM-revoke:* Now we discuss some more subtle details of the WSOM-revoke protocol. subtle details of the WSOM-revoke protocol.

Pre-selecting the join points To obtain a suitable set of Pre-selecting the join points To obtain a suitable set of join points, the joining node broadcasts in the local scope join points, the joining node broadcasts in the local scope a member request message. The member nodes that receive a member request message. The member nodes that receive the member request message reply a member reply message the member request message reply a member reply message including its identity and its distance to the data source. The including its identity and its distance to the data source. The joining node then selects the best join points among all the joining node then selects the best join points among all the member nodes who replied by considering the distance of the member nodes who replied by considering the distance of the replying member node to itself and to the data source. replying member node to itself and to the data source.

The size of the join point set In order to prevent arbitrary The size of the join point set In order to prevent arbitrary large join point set, which can potentially be used to mount large join point set, which can potentially be used to mount DoS attack during the revocation process and to delay the DoS attack during the revocation process and to delay the revocation of the node, the group manager can impose an upper bound on the number of join points each node can use. upper bound on the number of join points each node can use. Due to the static nature of the network topology, an upper Due to the static nature of the network topology, an upper bound as few as three can be sufficient. bound as few as three can be sufficient.

Handling group leaves Since group leave is a common event, Handling group leaves Since group leave is a common event, it is possible for a node that its actual join point decides to it is possible for a node that its actual join point decides to leave the group, or all the pre-selected join points of the node leave the group, or all the pre-selected join points of the node leave the group. In both cases, it is desirable that the ability leave the group. In both cases, it is desirable that the ability of the node to join the secure overlay is not affected. To of the node to join the secure overlay is not affected. To achieve this, we introduce a join point delegation mechanism. achieve this, we introduce a join point delegation mechanism. With the delegation mechanism, when a node decides to leave With the delegation mechanism, when a node decides to leave the group, it delegates the join point responsibility for its the group, it delegates the join point responsibility for its overlay children to its overlay parent by sending a signed delegation message to its overlay parent. Similarly, when a delegation message to its overlay parent. Similarly, when a node that has left the group receives join request, it delegates node that has left the group receives join request, it delegates the join point responsibility to its overlay parent with a signed the join point responsibility to its overlay parent with a signed delegation message. Therefore, in both cases, the joining node delegation message. Therefore, in both cases, the joining node can continue to join the secure overlay via the join point that can continue to join the secure overlay via the join point that has left; its ability to join the secure overlay is oblivious of has left; its ability to join the secure overlay is oblivious of the leave status of its selected join points. the leave status of its selected join points.

Updating join points It is possible that all of the pre-selected Updating join points It is possible that all of the pre-selected join points of a member node are revoked or fail. In such join points of a member node are revoked or fail. In such cases, it is necessary for the member node to obtain new join cases, it is necessary for the member node to obtain new join points in order to continue to participate in the secure overlay. points in order to continue to participate in the secure overlay. **A** member node may also desire to change its join point set if A member node may also desire to change its join point set if it finds a better set of join points. In both cases, a join point update procedure is called for. With WSOM-revoke, updating update procedure is called for. With WSOM-revoke, updating join points is achieved by obtaining a new member certificate join points is achieved by obtaining a new member certificate with the new join point set from the group manager. Since with the new join point set from the group manager. Since it is expected that the member revocation and failure events it is expected that the member revocation and failure events are infrequent and the static network environment limits the are infrequent and the static network environment limits the opportunity of finding better join points, we expect the join opportunity of finding better join points, we expect the join

¹ Delivering the revocation notice to the join points of the node is sufficient for denying the access to the group data for the node. The revocation notice for denying the access to the group data for the node. The revocation notice may also need to be delivered to the member nodes which have the revoked may also need to be delivered to the member nodes which have the revoked node as one of its join points, so that those nodes will not select the revoked node as one of its join points, so that those nodes will not select the revoked node as their overlay parent. However, under the assumption of no DoS attack, node as their overlay parent. However, under the assumption of no DoS attack, the revoked node cannot pretend to be member node to prevent member nodes' access to data. access to data.

point update procedure is only invoked infrequently, hence the point update procedure is only invoked infrequently, hence the centralized design for handling the procedure is acceptable. centralized design for handling the procedure is acceptable.

VII. ANALYTICAL COMPARISON VII. ANALYTICAL COMPARISON

In this section, we analyze and compare the overhead of In this section, we analyze and compare the overhead of the proposed protocols. We focus on the communication cost the proposed protocols. We focus on the communication cost since bandwidth is the main limitation. since bandwidth is the main limitation.

In order to have a clear comparison between the protocols, In order to have a clear comparison between the protocols, we make the following assumptions. We assume there is no we make the following assumptions. We assume there is no interference, thus the bandwidth cost for sending a message interference, thus the bandwidth cost for sending a message depends only on the path length (in hop count) and the size depends only on the path length (in hop count) and the size of the message. We use b to denote the bandwidth cost of transmitting one byte to the group via the multicast. Thus, the transmitting one byte to the group via the multicast. Thus, the bandwidth cost of multicasting a packet of size *D* to the group bandwidth cost of multicasting a packet of size D to the group is *bD.* We assume that the latency of a message depends only is *bD.* We assume that the latency of a message depends *only* on the number of hops travelled by the message and both join on the number of hops travelled by the message and both join and leave require only one round trip of message exchange. and leave require only one round trip of message exchange. Table I shows all the parameters we use in the comparison. Table I shows all the parameters we use in the comparison.

Table I1 shows the results of different metrics for different Table II shows the results of different metrics for different operations in the proposed protocols. Based on these compar-operations in the proposed protocols. Based on these comparison results, we now highlight a few differences between the ison results, we now highlight a few differences between the protocols. protocols.

For join and leave operations, there is potentially a large • For join and leave operations, there is potentially a large bandwidth and latency cost for W-LKH (depending on the bandwidth and latency cost for W-LKH (depending on the distance between the data source and the joining or leaving distance between the data source and the joining or leaving node), whereas, WSOM based schemes only incur constant node), whereas, WSOM based schemes only incur constant costs. costs.

W-LKH and WSOM-GK, which use the common group key • W-LKH and WSOM-GK, which use the common group key to encrypt group data, require rekey operations, whereas, no to encrypt group data, require rekey operations, whereas, no rekey operations are necessary for WSOM-LK and WSOM-HK. The rekey operations consume network bandwidth re-HK. The rekey operations consume network bandwidth resource, while batching introduces a vulnerability window. source, while batching introduces a vulnerability window.

WSOM based protocols require explicit revocation mes-• WSOM based protocols require explicit revocation messages, which is not necessary for W-LKH. In applications with only infrequent revocations, the bandwidth cost for revocation only infrequent revocations, the bandwidth cost for revocation is insignificant. For applications that require frequent revoca-is insignificant. For applications that require frequent revocations, we can batch process the revocations in the same way tions, we can batch process the revocations in the same way as batching the rekey operations for the group key and use the as batching the rekey operations for the group key and use the life time of membership certificates to reduce the revocation life time of membership certificates to reduce the revocation bandwidth overhead to an acceptable range. bandwidth overhead to an acceptable range.

For common group key based protocols (W-LKH and • For common group key based protocols (W-LKH and WSOM-GK), there is no per data packet overhead, whereas, WSOM-GK), there is no per data packet overhead, whereas, WSOM-LK and WSOM-HK incur per data packet overhead. WSOM-LK and WSOM-HK incur per data packet overhead.

VIII. EXPERIMENTAL EVALUATIONS VIII. EXPERIMENTAL EVALUATIONS

In this section, we present the results of our experiments In this section, we present the results of our experiments with the *ns* [13] network simulator for evaluating the proposed with the *ns* [13] network simulator for evaluating the proposed protocols. We first demonstrate the importance of reliable key protocols. We first demonstrate the importance of reliable key delivery for group key management protocols in WMNs, then delivery for group key management protocols in WMNs, then we evaluate and compare the performance and overhead of the we evaluate and compare the performance and overhead of the proposed protocols. proposed protocols.

A. Simulation Setup A. Simulation Setup

We implemented our experiments based on the *ns* network We implemented our experiments based on the *ns* network simulator [13] (version 2.26) with CMU Monarch extensions. simulator [13] (version 2.26) with CMU Monarch extensions. The MAODV implementation we used is provided by Zhu et The MAODV implementation we used is provided by Zhu et a1 [26]. al [26].

Nodes are configured to use the IEEE 802.1 1 radios with Nodes are configured to use the IEEE 802.11 radios with 2Mbps physical bandwidth and 250-meter nominal range. In 2Mbps physical bandwidth and 250-meter nominal range. In each simulation, 100 nodes are randomly placed within a 1500 each simulation, 100 nodes are randomly placed within a 1500 meters by 1500 meters area and the multicast data source is meters by 1500 meters area and the multicast data source is placed at the center of the area at the coordinates (750, 750). placed at the center of the area at the coordinates (750, 750).

The duration of a simulation is 900 seconds. In the begin-The duration of a simulation is 900 seconds. In the beginning of each simulation, a set of nodes are randomly selected ning of each simulation, a set of nodes are randomly selected to be the initial group members and join the group sequentially to be the initial group members and join the group sequentially at the rate of one join per three seconds. For experiments at the rate of one join per three seconds. For experiments with no group dynamics, the initial group size is the fixed with no group dynamics, the initial group size is the fixed group size for the experiment. For experiments with group group size for the experiment. For experiments with group dynamics, the initial group size is the stable group size for the dynamics, the initial group size is the stable group size for the experiment. After the initial joins are completed, the source experiment. After the initial joins are completed, the source starts to multicast data packets of size 256 bytes to the group starts to multicast data packets of size 256 bytes to the group at a rate specific to each experiment until the end of the at a rate specific to each experiment until the end of the simulation. For the experiments that examine the effect of simulation. For the experiments that examine the effect of group dynamics, the data rate is fixed at 5 packets/second.

Based on previously observed group dynamics for multicast Based on previously observed group dynamics for multicast applications [27], [28], [29], we use Poisson process to model applications [27], [28], [29], we use Poisson process to model the member join and leave events with different rates to reflect the member join and leave events with different rates to reflect different levels of group dynamics. We set the join and leave different levels of group dynamics. We set the join and leave rates to be equal, so the group size remains stable. For each join event, a random non-member node is selected to join the join event, a random non-member node is selected to join the group; similarly for each leave event, a random member node group; similarly for each leave event, a random member node is selected to leave the group. is selected to leave the group.

For protocols that require periodic rekeying (which includes For protocols that require periodic rekeying (which includes B-LKH, W-LKH and WSOM-GK), the rekey period is set to B-LKH, W-LKH and WSOM-GK), the rekey period is set to be 30 seconds. The maximum NACK timeout value used for be 30 seconds. The maximum NACK timeout value used for the reliable key delivery is set to be 100ms. We also assume the reliable key delivery is set to be lOOms. We also assume in all the protocols the size of symmetric keys is 128 bits, the in all the protocols the size of symmetric keys is 128 bits, the size of public/private keys is 1024 bits, and the computation delay for PKI signatures is 4ms .²

We experimented with different group sizes, however, since We experimented with different group sizes, however, since the comparison results of different protocols are similar for the comparison results of different protocols are similar for different group sizes, we only present the results for the group different group sizes, we only present the results for the group size of 50. In all the figures, each data point is the average of 10 different runs with different random topologies and of 10 different runs with different random topologies and different random group join and leave events. different random group join and leave events.

B. Metrics B. Metrics

We measure the performance of the secure multicast pro-We measure the performance of the secure multicast protocols with two metrics, the *delivery ratio* and the *decryption* tocols with two metrics, the *delivery ratio* and the *decryption ratio.* For each member node, the delivery ratio is defined *ratio.* For each member node, the delivery ratio is defined as the fraction of data packets that are received by the node as the fraction of data packets that are received by the node out of all the data packets that are broadcasted by the data source during the time when the node is a group member. source during the time when the node is a group member. The decryption ratio for a member node is defined as the The decryption ratio for a member node is defined as the fraction of data packets that can be decrypted by the member fraction of data packets that can be decrypted by the member out of all the data packets received by the member. Thus, out of all the data packets received by the member. Thus, the delivery ratio measures the impact of the secure multicast the delivery ratio measures the impact of the secure multicast protocol on the data delivery ability of the underlying multicast protocol on the data delivery ability of the underlying multicast

^{&#}x27;This value is based on the 1024 bits RSA implementation of openssl 2This value is based on the 1024 bits RSA implementation of openssl on **3GHz** Intel Pentium IV computer. on 3GHz Intel Pentium IV computer.

number of members	\boldsymbol{n}
multicast tree height	h
average tree degree	d
data packet size	D
symmetric key length	k
CRL length	\boldsymbol{r}
Total message size exchanged for	\mathcal{S}
join or leave	
distance between the joining or	δ
leaving node and the source	
bandwidth cost for group multicast	

TABLE I TABLE I PARAMETERS FOR PROTOCOL OVERHEAD ^aOne additional COMPARISONS COMPARISONS

		W-LKH	WSOM-GK	WSOM-LK	WSOM-HK
Join/Leave	bandwidth	δs			s+dk
	latency	2δ			3 ^a
Rekey	bandwidth	$bk \log n$	bdk		
	latency	п			
Revoke	bandwidth		br	bdr	$br + bk$
	latency		n	n	n
Data	bandwidth			bdk	bк
	latency	h	n	n	h
vulnerability window?		Yes	Yes	No	No

TABLE **I1** TABLE II OVERHEAD COMPARISON RESULTS OVERHEAD COMPARISON RESULTS α One additional hop time for the new link key

protocol, whereas, the decryption ratio measures the impact protocol, whereas, the decryption ratio measures the impact of the secure multicast protocol on the actual data goodput of the secure multicast protocol on the actual data goodput received by the upper layer application. In order to get a received by the upper layer application. In order to get a lower bound on the delivery ratio and the decryption ratio, lower bound on the delivery ratio and the decryption ratio, we assume the upper layer application requires time sensitive we assume the upper layer application requires time sensitive delivery, that is, a member node cannot buffer undecryptable delivery, that is, a member node cannot buffer undecryptable packets for decryption and forwarding upon the receiving of packets for decryption and forwarding upon the receiving of proper keys, instead such packets are dropped by the member. proper keys, instead such packets are dropped by the member.

The overhead of the secure multicast protocols are measured The overhead of the secure multicast protocols are measured in terms of the bandwidth overhead of the protocol and the in terms of the bandwidth overhead of the protocol and the latency for group join and leave events. Due to the scarcity latency for group join and leave events. Due to the scarcity of bandwidth resources on WMNs, it is essential to compare of bandwidth resources on WMNs, it is essential to compare the bandwidth overhead incurred by different protocols. The the bandwidth overhead incurred by different protocols. The latency of join and leave events reflects the responsiveness of latency of join and leave events reflects the responsiveness of the protocol to the upper layer applications. the protocol to the upper layer applications.

C. Reliable Key Transport C. *Reliable Key Transport*

We now demonstrate the importance of reliable key trans-We now demonstrate the importance of reliable key transport for secure multicast protocols on WMNs, which motivates port for secure multicast protocols on WMNs, which motivates our design for W-LKH. Figure $2(a)$ and $2(b)$ show the delivery and decryption ratio of LKH and B-LKH for different levels and decryption ratio of LKH and B-LKH for different levels of group dynamics. As we can see from these figures, while of group dynamics. As we can see from these figures, while both LKH and B-LKH maintain a similar delivery ratio as both LKH and B-LKH maintain a similar delivery ratio as the case without any security mechanism, these two protocols the case without any security mechanism, these two protocols have very poor decryption ratios. The poor decryption ratio for have very poor decryption ratios. The poor decryption ratio for LKH is due to two reasons: the high probability of key loss LKH is due to two reasons: the high probability of key loss on the wireless network and the frequent rekeying operations on the wireless network and the frequent rekeying operations which exacerbate the key loss problem. B-LKH improves which exacerbate the key loss problem. B-LKH improves the decryption ratio over LKH by reducing the frequency of the decryption ratio over LKH by reducing the frequency of the rekey operations, however, since the key loss problem is the rekey operations, however, since the key loss problem is not solved, the end result is still not satisfactory. If we can not solved, the end result is still not satisfactory. If we can further solve the key loss problem, as we will see in the further solve the key loss problem, as we will see in the performance results of W-LKH below, the decryption ratio performance results of W-LKH below, the decryption ratio turns out to be dramatically improved. Therefore, based on turns out to be dramatically improved. Therefore, based on these observations, we conclude that reliable key delivery is these observations, we conclude that reliable key delivery is essential for secure multicast protocols on WMNs. essential for secure multicast protocols on WMNs.

D. Protocol Performance and Robustness D. *Protocol Performance and Robustness*

Figure 2(c), 2(d) and Figure 2(e), 2(f) show the delivery and Figure 2(c), 2(d) and Figure 2(e), 2(f) show the delivery and decryption ratio for all the proposed protocols for different decryption ratio for all the proposed protocols for different levels of data rate and group dynamics, respectively. We ob-levels of data rate and group dynamics, respectively. We observe that for all the data rates and group dynamics examined, serve that for all the data rates and group dynamics examined, all the proposed secure multicast protocols can maintain a all the proposed secure multicast protocols can maintain a similar high delivery ratio as in the case where no security similar high delivery ratio as in the case where no security mechanisms are being used. The decryption ratios for all the mechanisms are being used. The decryption ratios for all the protocols are also almost 1. Therefore, we conclude that all protocols are also almost 1. Therefore, we conclude that all the proposed protocols can provide good transparency in terms the proposed protocols can provide good transparency in terms of data throughput to the upper layer applications. We also of data throughput to the upper layer applications. We also experimented with random node and link failures to examine experimented with random node and link failures to examine the robustness of the protocols in the case of failures. The the robustness of the protocols in the case of failures. The resulting performance is similar to the performance results shown for the case with no artificial failures. We omit these shown for the case with no artificial failures. We omit these graphs for the lack of space. graphs for the lack of space.

E. Protocol Overhead E. Protocol Overhead

I) Computation overhead: Figure 3(a) and3(b) show the *1) Computation overhead:* Figure 3(a) and3(b) show the computation overhead due to symmetric encryptions and computation overhead due to symmetric encryptions and asymmetric encryptions at the source node and a randomly asymmetric encryptions at the source node and a randomly selected member node for different protocols for experiments selected member node for different protocols for experiments with the data rate of 5 packets/second (10kbps) and the group dynamics of 5 joins and 5 leaves per minute. For the symmetric dynamics of 5 joins and 5 leaves per minute. For the symmetric encryption overhead, we observe that WSOM-LK has much encryption overhead, we observe that WSOM-LK has much higher overhead than the other protocols, especially at the higher overhead than the other protocols, especially at the source node. This is because WSOM-LK requires per data packet computation overhead that is linear to the number of packet computation overhead that is linear to the number of children of the node. For the asymmetric encryption overhead, children of the node. For the asymmetric encryption overhead, we observe that W-LKH has a significantly higher number of we observe that W-LKH has a significantly higher number of asymmetric encryptions performed at the source node than the asymmetric encryptions performed at the source node than the other protocols. The reason is that with W-LKH the source node handles all the join and leave requests, each of which node handles all the join and leave requests, each of which requires asymmetric encryption operations, whereas for the WSOM based protocols, the join and leave requests are han-WSOM based protocols, the join and leave requests are handled in a distributed fashion, hence the required asymmetric dled in a distributed fashion, hence the required asymmetric encryptions are shared by all member nodes. Since asymmetric encryptions are shared by all member nodes. Since asymmetric encryptions are computationally intensive operations, the high encryptions are computationally intensive operations, the high number of asymmetric encryptions at the source node in W-number of asymmetric encryptions at the source node in W-LKH can potentially introduce a performance bottleneck at the LKH can potentially introduce a performance bottleneck at the source, especially at high group dynamics. It also allows for source, especially at high group dynamics. It also allows for potential DoS attacks that aim at exhausting the computation potential DoS attacks that aim at exhausting the computation resource at the source node. resource at the source node.

2) *The bandwidth overhead and latency for join and leave 2) The bandwidth overhead and latency for join and leave operations:* Figure 3(c), 3(d) and Figure 3(e), 3(f) show the *operations:* Figure 3(c), 3(d) and Figure 3(e), 3(f) show the bandwidth overhead and latency for the join and leave events, bandwidth overhead and latency for the join and leave events, respectively, for different levels of group dynamics. From respectively, for different levels of group dynamics. From these graphs, we can make the following observations. First, these graphs, we can make the following observations. First, for all proposed protocols both the bandwidth overhead and for all proposed protocols both the bandwidth overhead and

latency remain stable for different levels of group dynamics. latency remain stable for different levels of group dynamics. Second, the WSOM based schemes have much less bandwidth Second, the WSOM based schemes have much less bandwidth overhead and latency than the W-LKH protocol for both join and leave events. This is the manifestation of the difference be-and leave events. This is the manifestation of the difference between the centralized and decentralized membership manage-tween the centralized and decentralized membership management principles. With decentralized membership management, ment principles. With decentralized membership management, as in the case of WSOM, only local messages are required for as in the case of WSOM, only local messages are required for joins and leaves. On the other hand, centralized membership joins and leaves. On the other hand, centralized membership management schemes, as W-LKH, require global messages management schemes, as W-LKH, require global messages

between the joining or leaving node to the data source. between the joining or leaving node to the data source.

3) *Peak bandwidth:* Figure 4(a), 4(b), 4(c), and 4(d) show *3) Peak bandwidth:* Figure 4(a), 4(b), 4(c), and 4(d) show the bandwidth consumed at the source node over time for all the bandwidth consumed at the source node over time for all the different protocols for a simulation run with the data rate the different protocols for a simulation run with the data rate of 5 packets/second (10kbps) and the group dynamics of 5 join and leave events per minute. From these graphs, we can join and leave events per minute. From these graphs, we can see that WSOM based protocols consume relatively stable bandwidth at the source over time, while W-LKH exhibits bandwidth at the source over time, while W-LKH exhibits high variability of bandwidth consumption. The reason for high variability of bandwidth consumption. The reason for

Fig. 4. The peak and total bandwidth overhead comparison Fig. 4. The peak and total bandwidth overhead comparison

the high peak bandwidth requirement of W-LKH is two-folds. the high peak bandwidth requirement of W-LKH is two-folds. First, the size of the rekey packets in W-LKH is relatively First, the size of the rekey packets in W-LKH is relatively large, since potentially many keys on the key tree needs to large, since potentially many keys on the key tree needs to be updated for a rekey event. Second, all the join and leave be updated for a rekey event. Second, all the join and leave requests require communication with the source in W-LKH. requests require communication with the source in W-LKH. Since high bandwidth peaks can cause packet loss and possible Since high bandwidth peaks can cause packet loss and possible congestions on the network, W-LKH is less favorable than the congestions on the network, W-LKH is less favorable than the WSOM based protocols in this respect. WSOM based protocols in this respect.

4) *Total bandwidth overhead:* In order to get an overview *4) Total bandwidth overhead:* In order to get an overview of all the bandwidth overhead introduced by the secure mul-of all the bandwidth overhead introduced by the secure multicast protocol, Figure 4(e) and 4(f) show the average total ticast protocol, Figure 4(e) and 4(f) show the average total bandwidth overhead due to the secure multicast protocol for bandwidth overhead due to the secure multicast protocol for an entire simulation session for different data rates and group an entire simulation session for different data rates and group dynamics, respectively. dynamics, respectively.

We first observe that the bandwidth overhead for both We first observe that the bandwidth overhead for both WSOM-LK and WSOM-HK increase linearly with the data WSOM-LK and WSOM-HK increase linearly with the data rate. However, the increase rate for WSOM-HK is significantly smaller than WSOM-LK, which makes the bandwidth overhead of WSOM-HK comparable to other protocols while the head of WSOM-HK comparable to other protocols while the bandwidth overhead of WSOM-LK are significantly higher. bandwidth overhead of WSOM-LK are significantly higher. This difference shows the effectiveness of the hop key in This difference shows the effectiveness of the hop key in WSOM-HK for reducing the bandwidth overhead. From Fig-WSOM-HK for reducing the bandwidth overhead. From Figure 4(f), we can also observe that for all the protocols, the total ure 4(f), we can also observe that for all the protocols, the total bandwidth overhead remains quite stable for different levels bandwidth overhead remains quite stable for different levels of group dynamics. of group dynamics.

F: Applicability of the Protocols F. Applicability of the Protocols

Based on the above experiment results, we now suggest *to appear in INFOCOM 2007*, 2007. Exact on the above experiment results, we now suggest [7] W. Du, J. Deng, Y. Han, and P. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE TDSC, vol. 3, applications with low dat since WSOM-HK has small join and leave latency and overall $[8]$ H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes bandwidth overhead and it does not have a vulnerability win-
[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for dow for forward and backward data secrecy. For applications and istributed sensor networks," in *Proc. of CCS '02*, 2002. applications with low data rate, WSOM-HK is the best choice,

with higher data rate, if the application can tolerate partial with higher data rate, if the application can tolerate partial loss for forward and backward data secrecy, then WSOM-GK loss for forward and backward data secrecy, then WSOM-GK is the best choice. Otherwise, neither W-LKH and WSOM-GK is the best choice. Otherwise, neither W-LKH and WSOM-GK can be used; the best choice is still WSOM-HK. can be used; the best choice is still WSOM-HK.

IX. CONCLUSION IX. CONCLUSION

In this paper, we explored different design choices for In this paper, we explored different design choices for solving the problem of secure multicast service for WMNs. solving the problem of secure multicast service for WMNs. We proposed several secure multicast protocols, and compared We proposed several secure multicast protocols, and compared them both analytically and experimentally. We discussed the them both analytically and experimentally. We discussed the trade-offs among different design choices and suggested the trade-offs among different design choices and suggested the best design choices for different application scenarios. Future best design choices for different application scenarios. Future work includes extending the proposed protocols to multi-work includes extending the proposed protocols to multisource group communications, and experimenting with the source group communications, and experimenting with the protocols in a wireless mesh testbed. protocols in a wireless mesh testbed.

REFERENCES

- [l] C. Wong, M. Gouda, and S. Lam, "Secure group communications using [1] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEWACM Traru. Netw.,* vol. *8,* no. 1, 2000. key graphs," *IEEElACM TrailS. Netw.,* vol. 8, no. 1,2000.
- [2] A. Perrig, D. Song, and I. D. Tygar, "Elk, a new protocol for efficient [2] A. Perrig, D. Song, and J. D. Tygar, "Elk, a new protocol for efficient large-group key distribution," in *Proc. of SBP,* 2001. large-group key distribution," in *Proc. of S&P, 2001.*
- [3] S. Mittra, "Iolus: a framework for scalable secure multicasting," in *Proc.* [3] S. Mittra, "Iolus: a framework for scalable secure multicasting," in *Proc. of ACM SIGCOMM '97,* 1997. *of ACM SIGCOMM* '97, 1997.
- [4] X. Zhang, S. Lam, and H. Liu, "Efficient Group Rekeying Using [4] X. Zhang, S. Lam, and H. Liu, "Efficient Group Rekeying Using Application Layer Multicast," in *Proc. of,ICDCS '05,* 2005. Application Layer Multicast," in *Proc. of ICDCS '05, 2005.*
- [5] C. Abad and I. Gupta, ""Adding confidentiality to application-level multicast by leveraging the muticast overlay"," *~roc.-if ADSN '05,* multicast by leveraging the muticast overlay"," in *Proc. of ADSN '05,* 2005. 2005. [5] C. Abad and I. Gupta, ""Adding confidentiality to application-level
- [61 R. Torres, X. Sun, A. Walters, C. Nita-Rotaru, and S. Rao, "Enabling [6] R. Torres, X. Sun, A. Walters, C. Nita-Rotaru, and S. Rao, "Enabling confidentiality of data delivery in an overlay broadcasting system," in *to appear in INFOCOM* 2007, 2007.
- [7] W. Du, J. Deng, Y. Han, and P. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE TDSC,* vol. 3, no. 1,2006.
- [8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of S&P, 2003.*
- [9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of CCS '02, 2002.*
- [lo] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "Gkmpan: An efficient group [10] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "Gkmpan: An efficient group rekeying scheme for secure multicast in ad-hoc networks," *Mobiquitous,* rekeying scheme for secure multicast in ad-hoc networks," *Mobiquitous,* vol. 00, 2004. vol. 00, 2004.
- [Ill R. Balachandran, B. Ramamurthy, X. Zou, and N. Vinodchandran, [II] R. Balachandran, B. Ramamurthy, X. Zou, and N. Yinodchandran, "Crtdh: an efficient key agreement scheme for secure group commu-"Crtdh: an efficient key agreement scheme for secure group communications in wireless ad hoc networks," in *Proc. of IEEE ICC '05,* 2005. nications in wireless ad hoc networks," in *Proc. ofIEEE ICC '05, 2005.*
- [12] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks," in *Proc. of SASN '03,* 2003. [12] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks," in *Proc. of SASN '03, 2003.*
- [I31 "The network simulator ns2." http://www.isi.edu/nsnam/ns/. [13] "The network simulator - ns2." http://www.isi.edu/nsnam/ns/.
- [I41 X. Li, Y. Yang, M. Gouda, and S. Lam, "Batch rekeying for secure group communications," in *Proc. of WWW '01,* 2001. [14] X. Li, Y. Yang, M. Gouda, and S. Lam, "Batch rekeying for secure group communications," in *Proc. of WWW '01, 2001.*
- [I51 C. Wong and S. Lam, "Keystone: A group key management service," in *Proc. of ICT '00,* 2000. *Proc. of ICT '00, 2000.* [15] C. Wong and S. Lam, "Keystone: A group key management service," in
- [I61 X. Zhang, S. Lam, D.-Y. Lee, and Y. Yang, "Protocol design for scalable [16] X. Zhang, S. Lam, D.-Y. Lee, and Y. Yang, "Protocol design for scalable and reliable group rekeying," *IEEE/ACM Trnru. Nerw.,* vol. 11, no. 6, and reliable group rekeying," *IEEEIACM Trans. Netw.,* vol. II, no. 6, 2003. 2003.
- [17] X. Zhang, S. Lam, and D.-Y. Lee, "Group rekeying with limited unicast [17] X. Zhang, S. Lam, and D.-Y. Lee, "Group rekeying with limited unicast recovery," *Comput. Networks,* vol. 44, no. 6, 2004. recovery," *Comput. Networks,* vol. 44, no. 6, 2004.
- [18] Y. Yang, X. Li, X. Zhang, and S. Lam, "Reliable group rekeying: a [18] Y. Yang, X. Li, X. Zhang, and S. Lam, "Reliable group rekeying: a performance analysis," in *Proc. of SIGCOMM '01,* 2001. performance analysis," in *Proc. of SIGCOMM '01, 2001.*
- [19] W.-P. Yiu and S.-H. Chan, "Sot: secure overlay tree for application layer [19] W-P. Yiu and S.-H. Chan, "Sot: secure overlay tree for application layer multicast," in *Proc. of ICC '04,* 2004. multicast," in *Proc. of ICC '04, 2004.*
- [20] C. Abad, I. Gupta, and W. Yurcik, "Adding confidentiality to application-[20] C. Abad, 1. Gupta, and W. Yurcik, "Adding confidentiality to applicationlevel multicast by leveraging the multicast overlay," in *Proc. of ADSN irl ICDCSW '05,* 2005. *in ICDCSW '05, 2005.*
- [21] S. Zhu, C. Yao, D. Liu, S. Setia, and S. Jajodia, "Efficient security [21] S. Zhu, C. Yao, D. Liu, S. Setia, and S. Jajodia, "Efficient security mechanisms for overlay multicast-based content distribution.," in *ACNS,* mechanisms for overlay multicast-based content distribution.," in *ACNS,* vol. 3531 of *Lecture Notes in CS*, pp. 40-55, 2005.
- [22] S. Roy, V. Addada, S. Setia, and S. Jajodia, "Securing maodv: Attacks [22] S. Roy, Y. Addada, S. Setia, and S. Jajodia, "Securing maodv: Attacks & countermeasures," in *Proc. of SECON '05,* 2005. & countermeasures," in *Proc. of SECON '05, 2005.*
- [23] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, 'The tesla broadcast [23] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes,* 2002. authentication protocol," *RSA CryptoBytes, 2002.*
- [24] E. Royer and C. Perkins, "Multicast operation of the ad-hoc on-demand [24] E. Royer and C. Perkins, "Multicast operation of the ad-hoc on-demand distance vector routing protocol," in *Mobile Cornputirzg nrzd Networking,* distance vector routing protocol," in *Mobile Computing and Networking,* 1999. 1999.
- [25] S. Pingali, D. Towsley, and J. Kurose, "A comparison of sender-[25] S. Pingali, D. Towsley, and J. Kurose, "A comparison of senderinitiated and receiver-initiated reliable multicast protocols," in *Proc. of* SIGMETRICS '94, 1994. *SIGMETRICS '94,* 1994.
- [26] Y. Zhu and T. Kunz, "MAODV implementation for NS-2.26," Technical [26] Y. Zhu and T. Kunz, "MAODY implementation for NS-2.26," Technical Report SCE-04-01, Carleton University. Report SCE-04-01, Carleton University.
- [27] K. Sripanidkulchai, A. Ganjam, B. Maggs, and H. Zhang, "The feasibil-[27] K. Sripanidkulchai, A. Ganjam, B. Maggs, and H. Zhang, "The feasibility of supporting large-scale live streaming applications with dynamic ity of supporting large-scale live streaming applications with dynamic application end-points,'' in *SIGCOMM,* 2004. application end-points," in *SIGCOMM, 2004.*
- [28] Y.-H. Chu, A. Ganjam, E. Ng, S. Rao, K. Sripanidkulchai, J. Zhan, and [28] Y.-H. Chu, A. Ganjam, E. Ng, S. Rao, K. Sripanidkulchai, 1. Zhan, and H. Zhang, "Early experience with an internet broadcast system based H. Zhang, "Early experience with an internet broadcast system based on overlay multicast," in *USENIX A111zun1 Teclzrlicnl Corfererzce,* 2004. on overlay multicast," in *USENIX Annual Technical Conference, 2004.*
- [29] K. Almeroth and M. Ammar, "Collecting and modeling the joinlleave [29] K. Almeroth and M. Ammar, "Collecting and modeling the join/leave behavior of multicast group members in the mbone," in *Proc. of (HPDC)* behavior of multicast group members in the mbone," in *Proc. of(HPDCj '96,* 1996. '96, 1996.

 $\ddot{}$