On a Low Security Overhead Mechanism for Secure Multi-path Routing Protocol in Wireless Mesh Network*

Muhammad Shoaib Siddiqui, Syed Obaid Amin, and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University,
Sochen-ri, Giheung-eup, Yongin-si, Gyeonggi-do, 446-701, South Korea
{shoaib,obaid}@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract. Secure multi-path routing is a critical issue in security management of WMNs due to its multi-hop nature as each node takes part in routing mechanism making it prone to routing attacks. Security management mechanisms are armed with features such as asymmetric cryptography which are costly in term of computations, transmissions and time delays. In this paper, we propose a security management mechanism for multi-path routing which efficiently uses the characteristics of WMNs, mutual authentication and secrete key cryptography to provide secure multi-path route management. Our management scheme takes less overhead than the available secure multi-path routing mechanisms. Simulation analyses and the performance of the mechanism are presented in support of the proposal.

Keywords: Security management, Secure multi-path routing, Wireless mesh networks, Security overhead, Public key cryptography.

1 Introduction

Wireless Mesh Network [1] is an emerging new technology which is being adopted as the wireless internetworking solution for the near future. Characteristics of WMN such as rapid deployment and self configuration make WMN suitable for transient on-demand network deployment scenarios such as disaster recovery, hard-to-wire buildings, conventional networks and friendly terrains. The form of mesh networks that are of most commercial interest are often called hybrid mesh networks [2], shown in Fig. 1. In hybrid mesh networks, the end users such as PDAs and laptops make up mesh client networks and mesh router nodes are part of the network infrastructure [2]. Here, the network consists of two types of links: short range wireless links (shown in Fig. 1 as dotted lines) among client mesh nodes and mesh relay links (shown in Fig. 1 as dashed lines) between router nodes to form the packet transport backbone.

WMN has been a field of active research in recent years. However, most of the research has been focused around various protocols for multi hop routing leaving the area of network and security management mostly unexplored. In this paper, we provide a management mechanism for hybrid wireless mesh networks, which reduces the security overhead in the network and in turns, increases the overall efficiency of

* "This paper was supported by ITRC and MIC".

S. Ata and C.S. Hong (Eds.): APNOMS 2007, LNCS 4773, pp. 466–475, 2007.

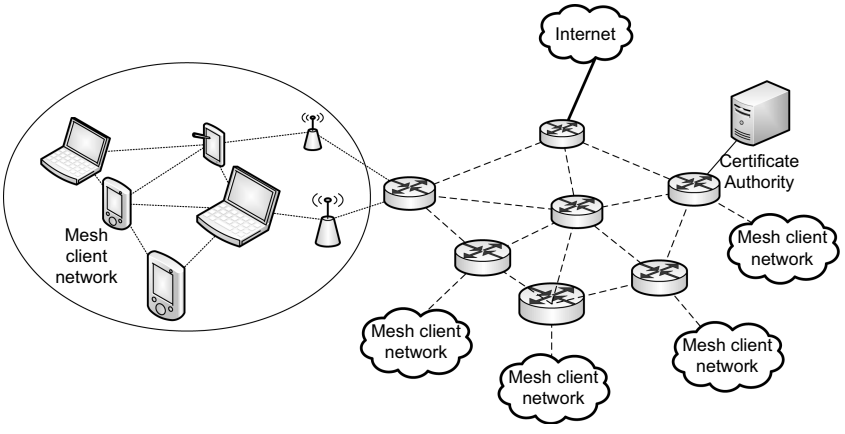

Fig. 1. A Hybrid Wireless Mesh Network

the secure routing protocol. In section 2, we discuss the various aspects of network management in WMNs with emphasis on security management. In section 3, we provide introduction to related approaches in the secure multi-path routing field. In section 4, we discuss the proposed management scheme. In section 5, we present the simulations and analytical comparison of our proposal with related work. In section 6, we conclude our proposal and discuss the future work.

2 Network Management

Network management refers to the maintenance and administration of large-scale computer and telecommunication networks at the top level. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring, maintaining and securing networks. The fundamental network management concepts in wireless mobile network are mobility management, route management, network monitoring and security management as shown in Fig. 2.

There are two ways of managing secure communication in WMNs: (1) Using the multiple paths [3] available in between the nodes. (2) Using the cryptographic key management to secure the communication in between two nodes. In first approach all the multiple paths between two nodes need to be node-disjoint (a node cannot participate in more than one path between two end nodes). If there are k multiple paths available then the adversary requires compromising at least k nodes – and more particularly at least one node in each path – in order to control the communication [4]. This approach is cost effective as it does not include any computation or transmission overhead and hardly inject delay in the network. But it does not ensure a certain level of security as there are not always multiple paths in between two end nodes and it is difficult to identify a compromised path.

Multi-path routing protocols need to be properly enhanced with cryptographic means which will guarantee the integrity of a routing path and the authenticity of the

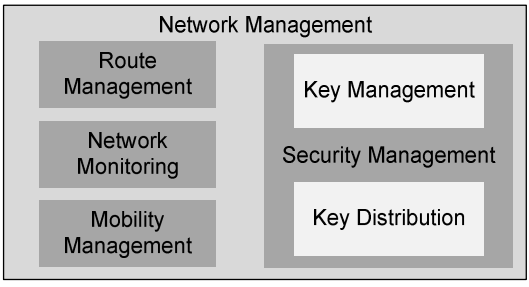

Fig. 2. Network management of the hybrid wireless mesh network

participating nodes. However, the cryptographic protection such as public key cryptography, increase the control and processing overhead and produce significant delay thus diminishing the efficiency of the secure multi-path routing protocol.

3 Related Works

Multi-path routing protocols [3] were initially designed for providing reliability [5] and QoS in the ad hoc networks. However, their nature of attack resilience was quickly identified as a significant security feature. Indeed, with single path routing protocols, it is easy for an adversary to launch routing attacks. A compromised node controlled by the adversary may participate in route discovery between end nodes without being noticed. Hence, the adversary can control the routing mechanism and disrupt the services at any instance.

Secure multi-path routing protocols are more resilient to routing attacks than typical routing protocols [6]. Although a lot of work is being done in the field of routing protocols in WMNs but little effort is put up for a security management in routing protocols. However, there are some protocols which are good enough to be implemented in WMNs and provide a secure multi-path route management such as [8], [7], [9] and [10].

A secure multi-path routing protocol called Secure Routing Protocol (SRP) [7] by Papadimitratos and Haas was initially developed considering the general security of ad hoc networks. Another approach was provided by Burmester and Van Le [8], which is based on the Ford-Fulkerson maximum flow algorithm. Kotzanikolaou et al presented Secure Multi-path Routing (SecMR) [10] protocol to reduce the cost of node authentication. SecMR works in two phases: mutual authentication and route discovery phase. At the end of route discovery, the end nodes use a symmetric key in order to verify the integrity of the discovered paths. SecMR provide multiple paths along with routing security and is better than the other two protocols. However, due to the use of digital signature in periodic mutual authentication phase, the computation cost and control overhead incurred render this scheme inefficient.

Michael Weeks and Gulshan Altan have provided a secure and efficient version of Dynamic Source Routing (DSR) in [9]. However, their security mechanism uses a shared network key, which is a single point of failure (if compromised), in the

network. There scheme also provide secured communication using public key cryptography, which again results in high computational cost and delay.

4 The Proposed Mechanism

Although wireless mesh networks are self organizing but they are also scalable and as the number of nodes increase in the network the size of the network makes network management essential. Network management helps in detecting abnormalities in the network and may help in other issues such as routing, guaranteeing QoS and providing security. Currently, to the best of our knowledge very little research has been done on the network management issues in wireless mesh networks. We provide a mechanism which makes network management simple and efficient.

4.1 Assumptions

Wireless mesh network has a hierarchical structure with mesh router making a routing infrastructure and mobile wireless clients making up ad hoc networks at the second level of the network. Each ad hoc network of wireless mesh clients has one or more routers from the router infrastructure in the ad hoc region. Our mechanism assumes that these router nodes are powerful enough to provide management functionality to the wireless mesh network. The routers which are connected to the mesh client nodes are named as boundary routers or manager routers. The mesh client networks are also termed as ad hoc regions/components. Nodes in the client mesh are also termed as client nodes (as shown in Fig. 1).

4.2 Mechanism

By associating each mesh client network with one router of infrastructure mesh, the management of the whole wireless mesh network would become simple. Each mesh client network can be managed by a boundary router. Boundary router is responsible of provide addresses, routing assistance, mobility management, power management and network monitoring to the mesh client networks. Security mechanism can also be enhanced by centralizing the mesh client network.

Route management is the job done by the routing protocol, while our mechanism provides security as an add-on to the existing routing protocol. Manager router in each mesh client provides the key management and distribution responsibilities. Manager router manages each mesh client network such as providing addresses, assisting routing and providing security. We also assume that there is a Certification Authority (CA) [11] in the wireless mesh network, which is a trusted third party that can authenticate the digital certificates of the nodes. Every node is provided with a pair of public and private key during the deployment phase.

With the implementation of this scheme, each mesh client network is now centrally managed by the manager router of that region. But the over all mesh network is still distributed. Each manager router communicates with other routers, collaborates and manages the whole wireless mesh network. We discuss the addressing, routing assistance, mobility management, routing assistance, network monitoring and security assistance by this mechanism.

4.3 Addressing and Mobility Management

Addresses for mobile clients are allocated dynamically by the router of that region. This address defines the location of the mobile client i.e. in which ad hoc region the mobile node is present. As the WMN clients are mobile, they may change position from one ad hoc region to the other. Our mechanism uses the techniques of Mobile IP [12] to provide addresses to client nodes. Similar to mobile IP, a client node has two addresses; one to identify it in its home ad hoc region and the other one is for the other ad hoc regions. Whenever a node enters the network for the first time, an address is assigned to it by the manager router. This router in the home (ad hoc) region of the client node serves the purpose of 'Home Agent'. When a client node changes it location and goes into another region, it is provided a second address from the router of that region. The client node informs its 'home agent' and its 'foreign agent' about this new address and location [12], so that a packet directed to the client node is redirected to its new address.

Hence, mobility of each client node can be easily managed. Locality information of each node is maintained by the manager routers. Whenever a node moves from one region to another region, the manager router of the new region provides new address to the node and the node remains connected to the network. The home agent directs the communicating node to the mobile nodes' new location.

4.4 Routing Assistance

Our mechanism also helps the routing mechanism. As the border router manages the addresses and monitors the network, it can help in routing decisions. The manager router can find optimal paths between two nodes, detect link losses and find alternate paths within the client mesh network. Network monitoring may keep a topological view which can also help in routing. Localization can help in geographic routing protocols by helping in decisions such as which neighbor node to forward the data to reach the destination node. The manager router can also work as a gateway between the static router infrastructure and the mobile client mesh network.

4.5 Network Monitoring

Due to dynamic nature of mesh clients, monitoring the network topology is a desired feature for WMNs. We can designate the responsibility of network monitoring of a single ad hoc region to a single manager router. Then all the client mesh networks can be monitored in a centralized way. These routers collaborate to perform the task of monitoring for the whole WMN in a distributed environment.

4.6 Security Management

Security is the most critical concern of every network. These days resource consuming public key cryptography is used to provide security which is not feasible for the client nodes. Our architecture presents an efficient way of reducing the security overhead.

Whenever a new node comes into a mesh client network, its request for an address is sent to the manager router of that region. The router provides the address to this

client node along with its public key and starts the process of mutual authentication with the node. The public key of the router node assures the authenticity and integrity of the following messages as all those messages are encrypted by the private key of the router node.

The client node and the router node encrypt the messages by their private keys before sending them to each other. This process authenticates both the nodes. For the authenticity of each other, the router node or the client node can contact the CA to verify the digital signature of each other. During this time of mutual authentication both nodes share a secret key using authenticated Diffie-Hellman [13] algorithm (shown in Algorithm 1) so that in the future they are not required to use public key cryptography. In the same way all the nodes within a mesh client network has a secret key shared by the manager router of that region. The algorithm is stated in the next sub-section.

The second phase is the key deployment phase among the client nodes. The router node distributes the keys calculated through a hash chain to all the client nodes for intercommunication. These are the secret keys which would be used by the client nodes to provide secure multi-path routing in the wireless mesh network.

4.7 Example

Let there be a wireless mesh network as shown in Fig. 3. The circle represents nodes and the dashed line shows the communication links. The cloud represents mesh infrastructure connected to several mesh clients. One such mesh client network is shown consisting of nodes **A**, **B**, **C**, **D**, and **R**. **R** is the router node managing the mesh client network while the other nodes are mesh client nodes. There is a **CA** connected to the mesh infrastructure somewhere in the wireless mesh network.

A new node **E** comes into the mesh client (shown in Fig. 3 as a grey node). First it sends an address request (such as DHCP request) in the network. The router node **R** provides the address to node **E**. After that they start the process of sharing a key using authenticated Diffie-Hellman.

At first, node **E** select two prime numbers g and p and a secrete integer a (e.g. $a=6$, $p=23$ and $g=5$) and calculate X and encrypt it with its own private key, make a digital signature and send it to node **R** along with p and g.

$$X = g^a \bmod p \;=\; 5^6 \bmod 23 \;=\; 8$$

R receives p, g and encrypted X and decrypts the message to get the value of X, using the public key of **E**. This authenticates the sender is **E**. **R** select an integer value b (e.g. $b=15$) and calculate Y, encrypt it with its own private key, make a digital signature and send it to **E**.

$$Y = g^b \bmod p \;=\; 5^{15} \bmod 23 \;=\; 19$$

E receives the encrypted Y and decrypts it using the public key of **R**. It then calculates the value of K.

$$K = [g^b \bmod p]^a \bmod p \;=\; Y^a \bmod p = 19^6 \bmod 23 = 2$$

Algorithm 1. The algorithm for authenticated Diffie-Hellman [13] for sharing a secret key between the router node R and the client node E is as follows:

Step 1. ***R*** *&* ***E*** *each possess a public/private key pair and a certificate for the public key.*
Step 2. ***R*** *&* ***E*** *agree to use a prime number p and g.*
Step 3. ***E*** *chooses a secret integer a, then sends* ***R*** *(g^a mod p) together with its signature and public key certificate.*
Step 4. ***R*** *chooses a secret integer b, then sends* ***E*** *(g^b mod p) together with its signature and public key certificate.*
Step 5. ***E*** *computes K = $(g^b \bmod p)^a \bmod p$*
Step 6. ***R*** *computes K = $(g^a \bmod p)^b \bmod p$*
Step 7. *Shared Secret key is K;* ***E****'s private key is 'a' and* ***R****'s private key is 'b'.*

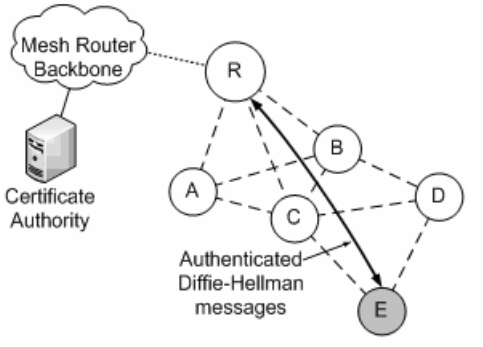

Fig. 3. Mutual authentication at the entrance of the node E in mesh client network

Similarly, **R** can calculate the value of *K*.

$$K = [g^a \bmod p]^b \bmod p \quad = X^b \bmod p = 8^{15} \bmod 23 = 2$$

5 Simulation and Analysis

We compared our security mechanism with the SRP [7], secure multi-path routing protocol of Burmester and Van Le [8] and SecMR [10] routing protocols. We perform the simulation of each of these security schemes. The proposed scheme is implemented with ad hoc on demand multi-path distance vector (AOMDV) [14] which is a multi-path derivative of AODV.

We have compared the routing overhead of these schemes and also the amount of energy consumed by these scheme at each node. We performed the simulation in NS-2 [15]. The network model was consisted of 49 client nodes placed randomly within an area of 1000 x 1000 m^2. There are 16 mobile router nodes deployed in a grid environment to make up the mesh infrastructure. This scenario constructed 10 different mobile client networks. Each node has a propagation range of 150 meters with channel capacity 2 Mbps. The speed of mobile nodes is set to be 0 or 20 m/s. The size of the data payload is 512. Each run of simulation is executed of 900 seconds of

simulation time. The medium access control protocol used is IEEE 802.11 DCF. The traffic used is constant bit rate (CBR).

5.1 Simulation Analysis

From Fig. 4 and Fig. 5, we observe that SRP works better than other schemes as it has less overhead and also consumes very little amount of energy. However, SRP does not provide optimal security; the intermediate nodes are not authenticated and the messages integrity is ensured by secret key cryptography. All this factors sum up to make SRP not feasible for wireless mesh networks.

The high routing overhead of scheme in [8] is due to the fact that it attaches the neighborhood information along with digital signatures with the route request and forward it towards the destination node. This information is increased at every node so the message size increases drastically and produces a huge amount of overhead. Although [8] is good for security and provides mutual authentication between the intermediate nodes as well as the end nodes but its overhead is very high; lot of energy is required at the client nodes and a share of bandwidth is wasted, plus delay in finding the route is also high.

SecMR protocol seems to be better than other schemes as it has less routing overhead and energy consumption than [8] and it also provides secure messaging. In SecMR, each node mutually authenticates its neighbor node at a periodic interval and public key cryptography is used to ensure security of the messages. Although the routing phase is separated from this authentication phase but this authentication is required after a constant interval, hence a considerable amount of energy is wasted in these periodic mutual authentications.

Our security mechanism does not require this periodic authentication, instead it uses public key cryptography only once and secret keys are used for further communication. This secret key deployment is not periodic and done after the mutual authentication by using public key cryptography. This reduces the energy consumption at each node and the routing overhead is also less than the other schemes.

5.2 Security Analysis

Our mechanism is secure enough that if a node is compromised then the whole network does not get affected by it. As all nodes communicates with each other with separate secret keys so, if a node is compromised and tries to adverse the network it is not possible for the node to be much hostile to the rest of the network. If there is a compromised node in the network, then there are two possibilities of an adversary node being in the network. In case 1, a node outside the network tries to attack the routing mechanism. Case 2 is the scenario in which the node entering the network is already a compromised node or the node is compromised during its participation in the network (such as due to the lack of physical protection etc).

In the first case, the messages by the compromised node would not be accepted by the other nodes as it cannot be authenticated by them. So the adverse messages would be dropped by the nodes as they cannot verify the adverse node as a member node.

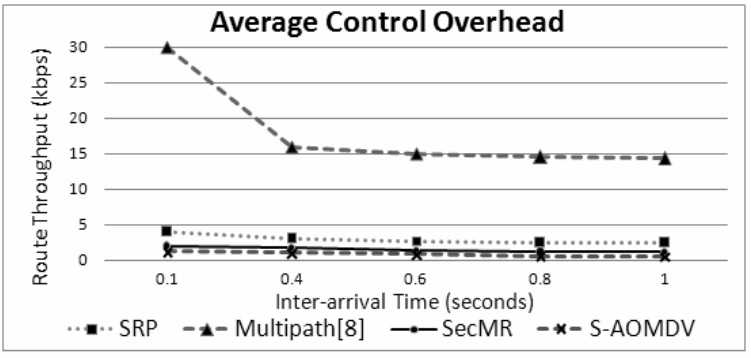

Fig. 4. Comparison of routing overhead of each protocol with function of time interval

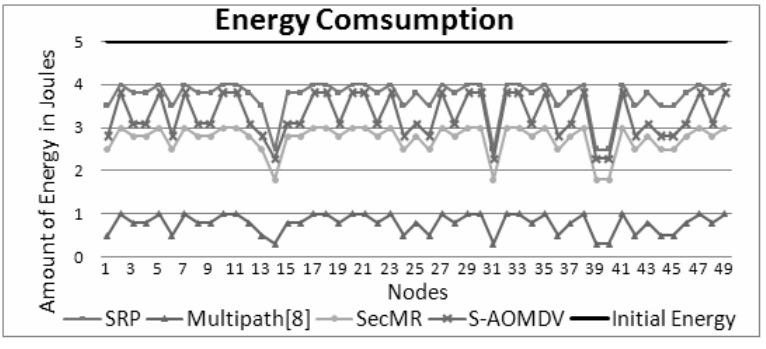

Fig. 5. Amount of energy left in joules at each node after the 900 s simulation

The second case can be harmful for the network as other nodes can verify the compromised node as a decent node. This node can communicate with its neighbor nodes and can inject false information in the network. But this compromised node cannot listen to other nodes' communications and cannot affect them. So if a node is compromised in the network all the other nodes are safe from this node and can communicate with other nodes securely. As our mechanism is for a multi-path routing protocol, hence, the messages are secure from the adversary as there are several paths to evade the compromised nodes. Even if the adversary have *'n'* compromised nodes with every compromised node is in a different path then with *'m'* paths in between two nodes, adversary require $n \geq m$.

6 Conclusion

In this paper, we have presented a security management mechanism for multi-path routing protocols in wireless mesh network. This scheme provides an efficient network management scheme, which enhances the life-time of the network as less energy is consumed in the network. Our security management scheme also sufficiently decreases the control overhead of a secure routing protocol. Currently, we

are working on this security mechanism to implement it in our multi-path routing protocol, which promises to provide better performance than AOMDV which we used for our simulations. This scheme is the basic efficiency factor in our secure multi-path routing protocol for wireless mesh networks.

References

1. Bruno, R., Conti, M., Gregori, E.: Mesh networks: commodity multihop ad hoc networks. IEEE Communications Magazine 43(3), 123–131 (2005)
2. Akyildiz, I.F., Wang, X., Wang, W.: Wireless Mesh Network: A Survey. Computer Networks and ISDN Systems 47(4) (2005)
3. Garcia-Luna-Aceves, J.J., Mosko, M.: Multipath Routing in Wireless Mesh Networks. In: WiMesh 2005, Santa Clara, CA, September 26, 2005, IEEE Computer Society Press, Los Alamitos (2005)
4. Gupta, R., Chi, E., Walrand, J.: Different Algorithms for Normal and Protection Paths. Journal of Network and Systems Management archive 13(1), 13–33 (2005)
5. Ganjali, Y., Keshavarzian, A.: Load Balancing in Ad hoc Networks: Single-path Routing vs. Multi-path Routing. In: proceedings of IEEE Annual Conference on Computer Communications (INFOCOM), 1120–1125 (March 2004)
6. Papadimitratos, P., Haas, Z.J.: Secure Routing for Mobile Ad Hoc Networks. Mobile Computing and Communications Review 6(4) (2002)
7. Papadimitratos, P., Haas, Z.: Secure routing for mobile ad hoc networks. In: Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), TX, San Antonio (January 2002)
8. Burmester, M., van Le, T.: Secure multipath communication in mobile ad hoc networks. In: ITCC 2004, IEEE, Las Vegas (2004)
9. Weeks, M., Altun, G.: Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks. Journal of Network and Systems Management 14(4), 559–581 (2006)
10. Kotzanikolaou, P., Mavropodi, R., Douligeris, C.: Secure multipath routing for mobile ad hoc networks. In: Proceedings of the WONSS05 Conference, St. Moritz, Switzerland, January 19-21 2005, pp. 89–96. IEEE, Los Alamitos (2005)
11. Raghani, S., Toshniwal, D., Joshi, R.: Dynamic Support for Distributed Certification Authority in Mobile Ad Hoc Networks. In: ICHIT 2006, vol. 1, pp. 424–432 (November 2006)
12. Perkins, C.E.: Mobile networking through Mobile IP. IEEE Internet Computing 2(1), 58–69 (1998)
13. Diffie, W., van Oorschot, P., Wiener, M.: Authentication and authenticated key exchange. Designs, Codes and Cryptography 2(2), 107–125 (1992)
14. Marina, M.K., Das, S.R.: On-demand multipath distance vector routing in ad hoc networks. In: the proceedings of Ninth International Conference on Network Protocols, November 11-14, 2001, pp. 14–23 (2001)
15. UCB/LBNL/VINT Network Simulator - ns 2, http://www.isi.edu/nsnamjns