Communications and Network, 2012, 4, **-**
Published Online February 2012 (http://www.SciRP.org/journal/cn)

A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks

Abdulrahman H. Altalhi
Information Technology Department, King Abdulaziz University, Jeddah, Saudi Arabia
Email: ahaltalhi@kau.edu.sa

Received 2012

ABSTRACT

A mobile ad hoc network (MANET) is a collection of mobile nodes that temporarily integrate with each other to form a network. Such a network does not require the existence of a typical network infrastructure. There is no central entity with the authority to administer the services and configurations of the network. How to secure a MANET is an active field of study for researchers. However, most of the research on the topic of securing the MANETs has focused on adapting security mechanisms that were meant for traditional wired networks. This adaptation has resulted in security solutions that do not work efficiently or that make assumptions that are not in line with the properties and characterizations of MANETs. In this paper, we propose the use of security mechanisms for MANETs that are designed based on the characteristics, functionalities, and goals of such networks. We aim to initiate a paradigm shift in securing MANETs, in which the focus should be on building security solutions specifically developed for MANETs, and not on adapting solutions that were meant for conventional wired networks. We revisit the basics and propose a simple encryption keys creation scheme that is based on the Diffie-Hellman key agreement protocol. The work presented in this paper should mark the initiation of a research agenda designed to build security primitives that are specifically for MANETs, along the lines of the new paradigm.

Keywords: Keys Management; MANET Security; Symmetric Encryption Keys

1. Introduction

The rapid progression of technology for mobile devices, including laptops and handheld computers, and the availability of inexpensive wireless networking hardware, has resulted in a great demand for wireless connectivity among mobile users. One approach to providing wireless connectivity is through the formation of a mobile ad hoc network (ad hoc, in Latin, means *for this only*).

A mobile ad hoc network (MANET) is a collection of mobile nodes that temporarily form a network. Such a network does not require the existence of the typical infrastructure underlying a network. Rather, each mobile node is equipped with a wireless interface that allows the node to communicate with other nodes via the wireless medium. Handheld computing devices and laptop computers with wireless transceivers are examples of mobile nodes that can come together to form a MANET. In a MANET, there is no central entity with the authority to administer the services and configurations of the network. All the nodes work collectively and cooperatively, in a distributed manner, to maintain the functions and services of the network. The distribution of responsibilities and tasks that are meant to keep the network running makes the network resilient to node failures. It also allows nodes to join and leave the network liberally without affecting the network's operability. One important challenge that the MANETs still face is providing secure communication between the nodes of a MANET.

2. Motivation

Before we introduce any security primitives, services, components, or protocols into a system, that system should be well understood and characterized. The aim should be to deploy security mechanisms that practically and efficiently integrate with the core characteristics and functionalities of the system at hand. This emphasis should be applied when we try to secure the communications within a MANET. The bulk of the research on securing MANETs has focused on adapting security mechanisms that were designed and developed for conventional wired networks. This adaptation has resulted in security solutions that do not work efficiently or that make assumptions that are not aligned with the characterization of MANETs. In this paper, we propose the use of security mechanisms for MANETs that are designed based on the characteristics, functionalities, and goals of

these networks.

The rest of this paper is organized as follows. In Section 3, we review the distinctive characteristics of ad hoc wireless networks. In Section 4, we elaborate on the requirements that must be fulfilled by candidate security frameworks for MANETs. A literature review of how to create encryption keys in the MANETs is presented in Section 5. The Diffie-Hellman key exchange [1], which is the basis for our proposed solution, is summarized in Section 6. Details of the proposed solution will be offered in Section 7. The paper is concluded in Section 8.

3. Characteristics of Mobile Ad Hoc Networks

MANETs have a number of distinctive characteristics that influence the design of security mechanisms to be utilized within them. In this section, we review some of these characteristics. A MANET is considered to be an autonomous self-organizing system of multiple mobile nodes that communicate wirelessly through the air. Nodes can join and leave the network at any time or at any state of the network. Additionally, nodes roam freely. There are no restrictions on the movements of the nodes. Such networks do not assume the existence of any supporting network infrastructure, nor do they require any prior setting up. The burden of providing networking services and functionality is handled cooperatively by the nodes of the network in a distributed fashion. We can summarize the discussed characteristics as follows [2]:

- Dynamic topologies of the network.
- Free mobility of the nodes.
- Limited processing power of the nodes.
- Limited storage capacity of the nodes.
- Limited power sources.
- No supporting infrastructure.
- No central authority to manage the network.
- No prior setting up.
- Distributed nature.
- Shared and open communication medium.

These characteristics should be taken into account while designing all the primitives, mechanisms, and protocols for securing the MANETs. Disregarding these characteristics or adapting modified ones may undermine the notion of an ad hoc network.

4. Security Requirements

Security frameworks for data communication must define a set of basic goals, services, and functionalities that enable the concerned parties to have secure communications. These services and functionalities constitute the building blocks for more complex security procedures and protocols. The frameworks in question should ensure that the requirements of *Integrity*, *Confidentiality*, *Authentication*, Non-*repudiation*, *Availability*, and *Access Control* are available to all communications [3-5]. Encryption is one of the key building blocks that facilitate the fulfillment of these requirements. We summarize the requirements as follows:

- *Integrity*:

  Communicated information should be protected from modification or alteration and tampering should be detectable.
- *Confidentiality*:

  Communicated information should be made accessible only to those who are authorized to receive it.
- *Authentication*:

  The identities of the parties involved in the information exchange should be verifiable.
- *Non-repudiation*:

  The actions of the parties involved in the information exchange should be undeniable.
- *Availability*:

  The system resources or services should be available to legitimate users as and when needed.
- *Access Control*:

  Unauthorized users should be prevented from accessing the system's resources or services.

5. Key Management and Previous Works

Communicating entities are said to have a *keying relationship* when they share keying material to support cryptographic procedures [6]. Establishing and maintaining a *keying relationship* through well defined procedures and methods is called *Key Management* [6]. Establishing the encryption key is a two step process [6]. The first step is that all the parties involved should agree on the key. The second step is to distribute the key to all the parties involved. Maintaining the encryption key involves procedures such as renewing or revoking the key. Cryptography is the central issue in cryptosystems, and *Key Management* is at the heart of cryptography. The policies and procedures of a *Key Management* system depend, among other things, on whether the type of the keys is *symmetric* or *asymmetric*.

In designing *Key Management* schemes for MANETs, designers should optimize the computational complexity, processing requirements, and storage space associated with such schemes. This is due to the limited resources of the nodes of the MANETs. Another aspect worth considering has to do with the connectivity conditions between the nodes. A MANET may become partitioned because of the mobility of the nodes. Interference patterns between two nodes may make the link between them a unidirectional one. We believe that a decentralized, lightweight, peer-to-peer *Key Management* scheme is the most suitable scheme for a MANET.

Securing the MANETs is an active field of research. Many solutions have been proposed and published that have advocated different approaches, which are based on different mechanisms and techniques. In this review, we focus on the notable items of work that represent the approaches that have been proposed so far. The solutions presented in [7-11] have adapted the traditional approach for wired networks that is based on *symmetric keys*. These solutions require a pre-deployment setup process which is not a characteristic of true ad hoc networking. In another approach that utilizes *asymmetric keys*, which was originally designed for wired networks, the solutions presented in [12-14] involve a high level of processing and communications. These solutions stress the resources of the nodes. One of the first attempts to preserve the ad hoc nature of the MANETs was demonstrated in [15]. However, that solution requires the nodes to come within the transmission ranges of each other to establish a *keying relationship*. In our proposed technique, we do not have such a requirement.

6. Diffie-Hellman Key Agreement Protocol

The solution we propose is based entirely on the pioneering work presented in [1], and is known as the Diffie-Hellman key agreement protocol. It was the first practical key distribution and creation protocol that permitted two communicating entities to create a shared key by exchanging information through an open channel, without requiring any prior knowledge to be shared among them [6]. This solution is a perfect match for the issues involved in forming a MANET. The security of this protocol is based on the computational hardness of the Diffie-Hellman problem and its related problem of calculating discreet logarithms [6]. The Diffie-Hellman protocol works as follows:

Assumption

G is a finite cyclic group with a generator g.

A and B are two entities who want to establish a shared secret key

Protocol Steps:

1) A secretly chooses integer S_A, at random, from the interval $[0, |G| - 1]$.

2) B secretly chooses integer S_B, at random, from the interval $[0, |G| - 1]$.

3) A computes $g^{S_A} \in G$.

4) B computes $g^{S_B} \in G$.

5) A sends g^{S_A} to B.

6) B sends g^{S_B} to A.

7) A computes $k = \left(g^{S_B}\right)^{S_A} = (g)^{S_B S_A}$.

8) B computes $k = \left(g^{S_A}\right)^{S_B} = (g)^{S_A S_B}$.

Since $(g)^{S_A S_B} = (g)^{S_B S_A}$, it follows that it can be used as a shared secret key.

7. Our Proposed Solution

When node A (to be called the initiator node) of a MANET wants to establish a shared encryption key with node B (to be called the target node), it chooses a prime number p, a base b, and a secret integer S_A. The initiator then calculates the value $V_A = b^{(S_A)} \ mod\ p$. After that, the initiator unicasts a Key Creation Message (*KC-Msg*) to the target node. The *KC-Msg* contains V_A, p, and b. Each node in the network maintains a simple data structure in the form of a table that is called a *Keys Table (KT)*. The *KT* consists of two columns. The first column is called the *Node ID*, and the second is called the *Key*. The purpose of this table is to keep track of any shared encryption keys that have been established with other nodes. When the initiator node sends the *KC-Msg*, it creates a tentative entry in the *KT* with values "Target Node ID" and "NULL", for *Node ID* and *Key* respectively.

Upon receiving the *KC-Msg*, the target node chooses a secret integer S_B and calculates the value $V_B = b^{S_B} \ mod\ p$. The target node then calculates the shared encryption key $K = V_A^{S_B} \ mod\ p$, and creates an entry in its *KT* with values "Initiator Node ID" and "*K*" for *Node ID* and *Key*, respectively. The final step of the protocol with respect to the target node is to send a Key Creation Response Message (*KCR-Msg*) that is unicasted to the initiator node. The *KCR-Msg* contains the V_B.

When the initiator node receives the *KCR-Msg*, it calculates the shared encryption key $K = V_B^{S_A} \ mod\ p$ and updates the *Key* field in the entry corresponding to the target node in its local *KT*. At this point, both of the nodes are in a position to start exchanging encrypted message using the newly created shard encryption key.

7.1. Informal Description

Creating the encryption key between node A and B can be informally described as follows:

1) Node A chooses a prime number p, a base b, and a secret integer S_A.

2) Node A calculates the value $V_A = b^{S_A} \ mod\ p$.

3) Node A sends the V_A, p, and b to node B.

4) Node B chooses a secret integer S_B.

5) Node B calculates the value $V_B = b^{S_B} \ mod\ p$ and sends it to A.

6) Node B calculates the shared encryption key $K = V_A^{S_B} \ mod\ p$.

7) Node A calculates the shared encryption key $K = V_B^{S_A} \ mod\ p$.

7.2. Formal Description

To describe the interaction between the nodes to create

the key, we will follow the conventional notation that is found in the cryptography literature. When the goal of principle *A* (node A) is to create a shared key with principle *B* (node B), a message *M* (base *b)*, a local secret key K_A (secret integer S_A), and modulus *n* (prime number *p*) are chosen such that *M* is a primitive root of *n* and $M < n$. Principle *A* then encrypts *M* using K_A with an encryption technique based on the exponentiation algorithm ($\{M\}_{K_A} = M^{K_A} \mod n$). The original message *M*, the encrypted *M*, and the modulus *n* are sent from principle *A* to principle *B*.

1) $A \rightarrow B$: $\{M\}_{K_A}, n, M$

Upon receiving *n* and *M*, principle *B* chooses a local secret key K_B and encrypts the message *M* with its own local key ($\{M\}_{K_B} = M^{K_B} \mod n$), which it then sends it to principle *A*.

2) $B \rightarrow A$: $\{M\}_{K_B}$

At this point, both principles can locally calculate the shared K_{AB} as follows:

3) In principle *A* $K_{AB} = \left(\{M\}_{K_B}\right)^{K_A} \mod n$

4) While in principle *B* $K_{AB} = \left(\{M\}_{K_A}\right)^{K_B} \mod n$

Both principles will reach exactly the same shared key (K_{AB}) with their local calculations. This is possible due the commutative property of exponentiation. That is, $\left((M)^{K_A}\right)^{K_B} \mod n = \left((M)^{K_B}\right)^{K_A} \mod n$. This property also allows for the interaction to create the shared key, which can be initiated by either principle. For an eavesdropper, the shard key (K_{AB}) is derived from known message (*M*) and modulus (*n*) but unknown local secret keys. If we use a very large prime for *n* and large numbers for K_A and K_B, it would be impossible to calculate the local keys of *A* and *B*.

7.3. Simple Example

We will illustrate how the protocol works with the following example:

1) Node *A* chooses $p = 31$, $b = 3$, $S_A = 4$.

2) Node *A* calculates $V_A = 3^4 \ mod\ 31 = 19$.

3) Node *A* sends $V_A = 19$, $p = 31$, and $b = 3$ to node *B*.

4) Node *B* chooses $S_B = 8$.

5) Node *B* calculates $V_B = 3^8 \ mod\ 31 = 20$; and sends it to node *A*.

6) Node *B* calculates $K = 19^8 \ mod\ 31 = 9$.

7) Node *A* calculates $K = 20^4 \ mod\ 31 = 9$.

7.4. Evaluation and Threats

Based on the previous description of our solution, creating the key would require the exchange of just two messages (*KC-Msg* and *KCR-Msg*). It would also require each node to maintain a very simple data structure (the *Keys Table KT*). We kept the requirements at a minimum to allow the solution to be efficiently used in MANETs.

The Diffie-Hellman protocol that we employed is primarily subject to two types of attacks: *brute force* and *man-in-the-middle* attacks. In a *brute force attack*, an attacker may exhaustively try all possible keys to decrypt an encrypted message. In [16], successfully performing such an attack would be equivalent to solving the *discrete logarithm problem.* This is a difficult problem. In a *man-in-the-middle* attack, a third malicious entity presents itself as a legitimate entity in the protocol exchange. For example, a malicious principle *C* can pretend to be principle *B* with regard to the exchange with principle *A* and pretend to be *A* with regard to *B*. This attack can be countered by utilizing the types of authentication services or protocols that are described in [17,18]. However, designing a new protocol for authentication that follows the principle of ad hoc wireless networking emphasized in this paper would be desirable. This is the next step in our future work.

8. Conclusion

In this paper, we introduced an encryption keys creation technique for MANETs based on The Diffie-Hellman key exchange. The technique is simple and preserves the ad hoc nature of MANETs. By publishing this work, we are trying to initiate a paradigm shift in securing MANETs. In the new paradigm that we are proposing, the focus should be on building security primitives purposely for MANETs, and not on adapting primitives that were meant for conventional wired networks.

REFERENCES

[1] W. Diffie and M. Hellman, "New Direction Ins in Cryptography," *IEEE Transaction on Information Theory*, Vol. IT-22, 1976, pp. 644-654. doi:10.1109/TIT.1976.1055638

[2] Y. Zhang, J. Zheng and M. Ma, "Handbook of Research on Wireless Security," *Information Science Reference*, Hershey, 2008. doi:10.4018/978-1-59904-899-4

[3] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Communications*, Vol. 11, No. 1, 2004, pp. 38-47. doi:10.1109/MWC.2004.1269716

[4] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," *Journal of Network and Computer Applications*, Vol. 30, No. 3, 2007, pp. 937-954. doi:10.1016/j.jnca.2005.07.008

[5] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks," In: J. Chen and J. Wu, Eds., *Handbook of Research on Developments and Trends in Wireless Sensor Networks*: *From Principle to Practice*, IGI Global,

Hershey, 2010, pp. 262-289. doi:10.4018/978-1-61520-701-5.ch012

[6] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1996. doi:10.1201/9781439821916

[7] H. Luo and S. Lu, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, Vol. 12, No. 6, 2004, pp. 1049-1063. doi:10.1109/TNET.2004.838598

[8] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks," *Proceedings of the* 1*st Annual International Conference on Mobile and Ubiquitous Systems*: *Networking and Services* (*MobiQuitous*'04), Boston, 22-25 August 2004, pp. 52-61.

[9] D. Liu, P. Ning and W. Du, "Group-Based Key Predistribution for Wireless Sensor Networks," *ACM Transactions on Sensor Networks* (*TOSN*), Vol. 4, No. 2, 2008, pp. 1-30. doi:10.1145/1340771.1340777

[10] B. Wu, J. Wu, E. Fernandez and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," *Proceedings of the* 19*th IEEE International Parallel and Distributed Processing Symposium* (*IPDPS*' 05), *Workshop* 17, Denver, Vol. 18, 3-8April 2005.

[11] S. Capkun, L. Buttya and P. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," *IEEE Transaction on Mobile Computing*, Vol. 2, No. 1, 2003, pp. 52-64. doi:10.1109/TMC.2003.1195151

[12] A. C.-F. Chan, "Distributed Symmetric Key Management for Mobile Ad Hoc Networks," *Proceedings of the* 23*rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Hong Kong, Vol. 4, 7-11 March 2004, pp. 2414-2424.

[13] R. Novales and N. Mittal, "Parameterized Key Assignment for Confidential Communication in Wireless Networks," *Ad Hoc Networks*, Vol. 9, No. 7, 2011, pp. 1186-1201. doi:10.1016/j.adhoc.2011.01.009

[14] J. Lee and D. R. Stinson, "On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs," *ACM Transactions on Information and System Security* (*TISSEC*), Vol. 11, No. 2, 2008, pp. 1-35. doi:10.1145/1330332.1330333

[15] S. Capkun, J. Hubaux and L. Buttyan, "Mobility Helps Peer-To-Peer Security," *IEEE Transactions on Mobile Computing*, Vol. 5, No. 1, 2006, pp. 43-51. doi:10.1109/TMC.2006.12

[16] E. Bresson, O. Chevassut and D. Pointcheval, "The Group Diffie-Hellman Problems," In: K. Nyberg and H. Heys, Eds., 9*th Annual International Workshop on Selected Areas in Cryptography* (*SAC*'02), Springer-Verlag, London, 2002, pp. 325-338.

[17] E. Ngai, M. Lyu and R. Chin, "An Authentication Service against Dishonest Users in Mobile Ad Hoc Networks," *Proceedings of the* 2004 *IEEE Aerospace Conference*, Big Sky, Vol. 2, 6-13March 2004, pp. 1275-1285.

[18] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A Lightweight Network Access Control Protocol for Ad Hoc Networks," *Ad Hoc Networks*, Vol. 4, No. 5, 2006, pp. 567-585. doi:10.1016/j.adhoc.2005.06.002

