Mobile Ad-Hoc Network Security: An Overview

Md. Majharul Haque¹, Md. Shakil Ahamed Shohag², Abu Sadat Mohammed Yasin³, Sadia Binte Anwar⁴

¹University of Dhaka, Bangladesh
²University of Development Alternative, Bangladesh
³Shahjalal University of Science and Technology, Bangladesh
⁴World University, Bangladesh

ABSTRACT
In the golden era of modern science, the explosive expansion of mobile computing devices, which principally take into account laptops, personnel digital assistants (PDAs), handheld digital devices and etc., has incited a revolutionary amendment to the computing world. Thus the ubiquitous computing environment has been formed, which is wireless Mobile Ad Hoc Network and attracted most concentrations from many proficient researchers. But Mobile Ad Hoc Networks have far more vulnerabilities because of security threat, which is very much hard to maintained comparing to wired networks. Endeavour of so many researchers is yet to be finished for the innovation of a secured framework for Mobile Ad Hoc Network (MANET). In this paper, different security aspects of wireless networks are addressed and diversified methodologies of various researchers are discussed from the very beginning of this research to this modern age. The effort has been given here to observe the trends of numerous security standards. Also some promising approaches are indicated and particular concentration is devoted for the scrutinizing a range of procedure from raw level to high professional, so that in future one can get precious guideline for further betterment. Furthermore, the related work on this arena will give a paradigm of challenges and explore the scopes for research work in depth of wireless security.

Keyword - Mobile computing, Ad-Hoc Network, wireless networks, security standards, wireless security

1. INTRODUCTION
A Mobile Ad Hoc Network (MANET) is an infrastructure-less special wireless network of mobile devices where each device acts as a router. The Latin term Ad Hoc means For the Specific Purpose. Ad Hoc networks are instantly formed to serve a specific purpose and cease to exist after the network fulfills its purpose. MANET is a self-configuring network connected by wireless links. Most Ad Hoc networks do not rely on any underlying fixed infrastructure such as base stations or access points. Instead, mobile hosts (or nodes) rely on each other to keep the network connected depicted in fig. 1. Each device in MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each node must forward traffic to make the network consistent. Therefore, every node in MANET is treated as a router.

Some MANETs are limited to a small or local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network) is a type of MANET that allows vehicles to communicate with roadside equipment. In this situation the vehicles may not have a direct internet connection. The wireless roadside equipment may be connected to the internet, allowing data from the vehicles to be sent over the internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

In this paper, a brief description of background knowledge and previous research works on Wireless Ad hoc Network Security has been provided.
The rest of the paper is organized as follows: background knowledge is provided in section 2. Section 3 presents a comprehensive literature review about different procedures of ensuring security in mobile ad hoc network. At a glance comparison among the various methods is illustrated in section 4. Section 5 turns conclusion with a brief about this paper.

2. BACKGROUND

The increased popularity of ad hoc network requires the prevention of adversaries attempting to jeopardize the network operation. Security is very important concern for wireless networks. The four major issues regarding security are Confidentiality, Authentication, Integrity and Non Repudiation. Confidentiality [1] issue ensures that the data transmitted through communication medium should not be eavesdropped. Authentication [1] issue concerns with the access of information by only legitimate users in the network. Integrity [1] issue ensures that the transmitted message has not been tampered by any intruders. Finally, Non Repudiation [2] ensures that neither the sender nor the receiver can deny the transmission or acceptance of the information.
A big challenge has been thrown to system security designers regarding the nature of ad hoc network due to the following reasons, those are not limited to:

- The wireless networks are so vulnerable to attacks ranging from passive eavesdropping to active interfacing.
- Mobile devices usually have limited power consumption as well as computational capabilities for which they are so susceptible to Denial of Service (DoS) attacks and unable to execute computation-heavy algorithms like public key algorithms.
- Frequent network/networking reconfiguration is enforced which facilitates more attacks to be launched. For example, differentiation between state routing information and faked routing information is hard.
- The lack of online Certificate Authority (CA) or Trusted Third Party (TTP) creates more difficulty for deploying security mechanisms.
- In MANETs, there are awful probabilities of being compromised for trusted nodes and then be used by adversary to launch attacks on the networks. Consequently, designers have to deal with both insider attacks and outsider attacks in MANETs, where insider attacks are more difficult to handle.

3. REVIEW ON THE SECURITY ON MOBILE NETWORK

In the very beginning of the research in the ground of wireless communication, security was a great challenge. Ensuring bullet proof jacket for the robust security concern is yet to be in reality. But so many researchers have been trying to establish a secured framework for safe and sound communication in mobile ad hoc network. There are a lot of interesting publications, projects in this field as this is a burning topic in our daily life. Here is an overview on them with indicating significant points.

3.01 Donald Welch et al. [3] in 2003
The authors surveyed over various wireless security threats and their counter measures cryptographic techniques. They categorized the threats based on different security issues. Traffic analysis, passive eavesdropping, and active eavesdropping are three classified attacks that violate confidentiality or privacy of the session. The man-in-the-middle attack defies both confidentiality and integrity. The rest three attacks, namely unauthorized access, session hijacking and the replay attack breach the integrity of the network traffic. For the counter measures, the researchers proposed to find an integrated secure framework having suitable authentication mechanism along with a strong and secure encryption algorithm using block cipher.

3.02 Ravi K. Balachandran et al. [4] in 2005
They suggested an efficient key agreement scheme namely Chinese Remainder Theorem and Diffie-Hellman (CRTDH). According to this CRTDH, there is no pre-shared secrecy between the members and the service of a trusted authority or a group controller is not required. CRTDH uses the Diffie-Hellman key exchange and the Chinese Remainder Theorem for efficient key agreement of Symmetric Cipher. Member serialization and central authority are two major problems of SGC scheme which are solved by CRTDH. Uniform workload distribution for all the members, efficient computation of group key and few rounds of re-keying are more accentuated by this protocol. However, CRTDH suffers from man-in-the-middle attack; also it is not optimized for a scalable ad hoc network. The CRTDH relies more on the verification of SSS to become successful [5].

3.03 Mahalingam Ramkumar et al. [6] in 2005
Authors suggested Hashed Random Preloaded Subsets (HARPS), a novel identity based pre-distribution model. They made a composition of two Probabilistic KPDs namely, Random Pre-distribution Scheme (RPS) and Leighton and Micali Scheme (LM) in their key Pre-distribution Scheme (KPD). A cryptographic hash function h(.) for one way encryption and a public-key-generation function F(.) for greater security were proposed in their paper. HARPS is defined by three parameters (P, K, L). The Trusted Authority (TA) determines P secrets or root keys. From each root key one can get L derived keys by repeated application of the one-way function h(.) for a
node of identity ID_A, application of public function F(ID_A) yielded a sequence of K length ordered pairs. According to this scheme all nodes are preloaded initially with K secrets, so that authenticated secret sharing can be ensured. Although the approach is novel, there remain some major drawbacks of the scheme. HARPS uses PKI over symmetric key cryptography which increases overhead of the system. Since the entry and exit of a node in MANET is not fixed, Calculation and Key Pre-distribution are not feasible [7]. Furthermore it is not discussed in this model that how the system manages the keys of leaving nodes.

3.04 Tina Suen et al. [8] in 2005
They concentrated on identification and authentication in ad hoc networks. Identification and authentication are particularly susceptible to identity attacks, for example, masquerading. For mitigating the identity attacks, they proposed to associate the message transmitter with a location and use this location information to find out identity. According to the proposed method, a Verifying Node (VN) authenticates a transmitting peer node’s location using a combination of signal properties, trusted-peer collaboration, and global positioning systems (GPS) for identification purposes. Although they emphasized in the direction information about peer identity from signal’s origin, signal direction by itself is not a strong identity indicator. Moreover, they consider identification based on triangular positioning system where the three key points are The VN, trusted peer, and transmitter. Then, triangulation and trigonometric functions are used to calculate the transmitter’s location. But a problem occurs when the three points lied on a same straight line. Moreover, calculation based on relative position is not an efficient approach for identifying a deceptive node.

3.05 Shichun Pang et al. [9] in 2006
They introduced an optimized vector space verifiable SSS. The security of their proposed model is based on Elliptic Curve Cryptography (ECC) [10]. The model had precondition of (t, n) threshold SSS. A verifiable infrastructure provided in this paper detects the cheats from assignee and dealer. The shared key distributed by dealer is encrypted based on ECC. It is claimed that the communication and computation cost for their suggested mode is less than any existing SSS. The key of elliptic curve cryptography has the length which is much less than RSA cryptography. Therefore, the model should be so important in applications with limited computing power and memory.

3.06 Clare McGrath et al. [11] in 2006
They proposed different key management techniques. For efficient key management for MANET, they identified many challenges and research options in their paper. It was suggested here that the asymmetric key encryption is more secure and flexible than symmetric key encryption. Finally, emphasized to use such a PKI protocol that may help computation, communication, memory used and power restrictions of MANET.

3.07 Wei Liu et al. [12] in 2006
They drew attention to ID-based Key Management (IKM) cryptography. IKM as a certificate-less solution helps public keys of mobile nodes to be directly derivable using their known IDs and some common information. Consequently, it removes the necessity of certificate-based authenticated public-key distribution, which is essential in conventional public-key management schemes. Even though the researchers claimed based on their simulation result that, IKM is more efficient and optimized as compared to conventional certificate based authorization; but without any single certificate key generation authority like Kerberos, the unique generation of ID for a distributed system is very hard.

3.08 PI Jian-Yong et al. [13] in 2006
They studied a scheme to discard the traditional identity authentication mechanism for identity and PKI. Compared with the key of session, the identity of each node in Ad Hoc network is fixed. The authentication code (AC) remains unchanged in all sessions and the session key is different in every session. Their performance analysis shows that, existential forgery attacks and Byzantine node conspiracy attacks can be prevented by their
scheme. Although the simulation results of the proposed cryptography exacted high efficiency against Sybil Attack, the scheme is susceptible to the key replicating attack [14].

They suggested an application domain specific detection mechanism for mobile ad hoc networks. The scheme is based on the fact that Sybil nodes in Mobile Ad Hoc Networks normally move in clusters. The researchers showed that the evaluation of geographical location patterns of clusters of identifiers, which are moving together, can potentially indicate the presence of a device launching a Sybil attack. The scheme did not consider the multiple collaborating Sybil attackers that can thwart observer’s node and can cause Denial of Service (DoS).

3.10 Marianne A. Azer et al. [16] in 2007
They studied different threshold cryptography techniques and SSS. In their paper, they enlisted many challenges along with research options in the field of threshold cryptography and authentication. The major challenges of SSS are validity period of the partial key or secret sharing, selections of the optimum threshold level, dynamic adjustment of the partial key validity time and behavior of corrupted nodes using incorrect partial keys.

3.11 Pierre E. Abi-Char et al. [17] in 2007
They surveyed over a secure authenticated key agreement protocol based on ECC. The model provides secure mutual authentication and explicit key establishment over an insecure network. They claimed that the proposed model is more secure than any other existing Simple Key Agreement (SKA) protocols. Their model resists from man-in-the-middle attack, know-key and resilience to server attack along with the dictionary attacks mounted by either passive or active network intruders. The proposed protocol uses the signature techniques of ECDSA and the SKA protocol concept. Furthermore, the communication and computation cost of the model has been reduced greatly from other SKA protocols.

They introduced Address-based Cryptography Scheme (ACS) as a security model for MANET. ACS is a combination of public key cryptography and Ad hoc node address. Unlike other certificate based cryptography, ACS nodes are directly deliverable from their known Ad hoc node address and some common information such as number of nodes in the network, entry time and exit time. They demanded that in their proposed framework MANETs are protected from the eavesdropping and masquerading. The private and public key generation in ACS does not ensure uniform key distribution, which is essential for enhancing security in public key cryptography. ACS broadcasts encrypted message containing its own private key which increases security threats for MANET.

3.13 Mengbo Hou et al. [14] in 2009
They proposed that ID based cryptography scheme is susceptible to the key replicating attack, which is one form of man-in-the-middle attack, where an active adversary can intercept and properly modify the messages exchanged between two parties, and force the two parties to accept the same session key; however that is not a state to be agreed on it for both parties.

3.14 Yuguang Fang et al. [19] in 2009
They introduced different cryptographic techniques for wireless Ad-hoc networks. They suggested to employ Identity Based Cryptography [20], considering the limited resource constraints of MANET. Although the excessive overhead of key agreement from CA is reduced by the Identity Based Public Key Cryptography (ID-PKC), the security of ID-PKC depends on the difficulty of computing Bilinear Diffie-Hellman Problem (BDHP).
4. COMPARISON AMONG THE PROCEDURES

At a glance comparison among the discussed techniques of security in mobile ad-hoc network has been shown in table 1.

<table>
<thead>
<tr>
<th>#</th>
<th>Author(s), Year, Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Donald Welch, 2003, [3]</td>
<td>This paper has a survey over various wireless security threats like traffic analysis, passive eavesdropping, active eavesdropping, man-in-the-middle, unauthorized access, session hijacking and the replay attack. An integrated secure framework having suitable authentication mechanism along with a strong and secure encryption algorithm using block cipher have been proposed for counter measures.</td>
</tr>
<tr>
<td>2</td>
<td>Ravi K. Balachandran, 2005, [4]</td>
<td>In this paper CRTDH key agreement scheme has been proposed for which there is no pre-shared secrecy between the members and the service of a trusted authority or a group controller is not required. CRTDH suffers from man-in-the-middle attack; also it is not optimized for a scalable ad hoc network and it relies more on the verification of SSS to become successful [5].</td>
</tr>
<tr>
<td>3</td>
<td>Mahalingam Ramkumar, 2005, [6]</td>
<td>The new method invented here named Hashed Random Preloaded Subsets (HARPS), where all nodes are preloaded initially with k secrets so that authenticated secret sharing can be assured. HARPS uses PKI over symmetric key cryptography which increases overhead of the system. Since the entry and exit of a node in MANET is not fixed, Calculation and Key Pre-distribution and in MANET is not viable [7].</td>
</tr>
<tr>
<td>4</td>
<td>Tina Suen, 2005, [8]</td>
<td>According to the proposed method, a Verifying Node (VN) authenticates a transmitting peer node’s location using a combination of signal properties, trusted-peer collaboration, and global positioning systems (GPS) for identification purposes. However calculation based on relative position is not an efficient approach for identifying a deceptive node.</td>
</tr>
<tr>
<td>5</td>
<td>Shichun Pang, 2006, [9]</td>
<td>A verifiable infrastructure provided in this paper detects the cheats from assignee and dealer. It is claimed that the communication and computation cost for their suggested mode is less than any existing SSS. The model should be so important in applications with limited computing power and memory.</td>
</tr>
<tr>
<td>6</td>
<td>Clare McGrath, 2006, [11]</td>
<td>A different type of key management technique has been proposed here. It is suggested here that the asymmetric key encryption is more secure and flexible than symmetric key encryption.</td>
</tr>
<tr>
<td>7</td>
<td>Wei Liu, 2006, [12]</td>
<td>An ID-based Key Management (IKM) system introduced to eliminate the need for certificate-based authenticated public-key distribution indispensable in conventional public-key management schemes; but the unique generation of ID for a</td>
</tr>
</tbody>
</table>
5. CONCLUSION

In this research work the concepts of Mobile Ad Hoc Network’s security with various aspects have been reviewed that categorize different approaches in this ground. Vulnerability issues are clearly emphasized here in this literature review. Recent trend of the procedure of wireless security that comes from novice to high professional has been scrutinized here. It can be said boldly that the study of wireless security is a productive region for further research because of its’ exposed structure and worldwide demand. Around 14 paper have been briefly discussed and various key topics from other historical publication relevant with structure less network’ protection have been analyzed from the very beginning of the commencement of research in this dome. Nowadays, in the age of mobile network, information is being shared from point to point in everywhere mostly by wireless media and the wired network is going to be in museum. So the research about the security of mobile ad-hoc network is a burning issue. After all we have faith that any researchers can get help from this literature review for better understanding of different sorts of wireless security procedure. It will be also supportive for better perception of the diversified types of protection method, which will assist in construction of new formula and systems that considerably serve the various principle for giving security in broad-spectrum.
REFERENCES


