A Novel Technique Based on Node Registration in MANETs

Rashid Jalal Qureshi[1],Khalid Haseeb[2],Muhammad Arshad[3] , Huma Javed[4],Haleem Farman[5]

[1,2] Islamia College Peshawar (Chartered University)
Peshawar, Pakistan

[3] City University of Science and Information Technology
Peshawar, Pakistan

[4,5] University of Peshawar, Pakistan

Abstract

In ad hoc network communication links between the nodes are wireless and each node acts as a router for the other node and packet is forward from one node to other. This type of networks helps in solving challenges and problems that may arise in every day communication. Mobile Ad Hoc Networks is a new field of research and it is particularly useful in situations where network infrastructure is costly. Protecting MANETs from security threats is a challenging task because of the MANETs dynamic topology. Every node in a MANETs is independent and is free to move in any direction, therefore change its connections to other nodes frequently. Due to its decentralized nature different types of attacks can be occur. The aim of this research paper is to investigate different MANETs security attacks and proposed nodes registration based technique by using cryptography functions.

Keywords: *Mobile Adhoc Network*, network security, malicious node detection, cryptography techniques.

1. Introduction

MANET is an infrastructure less network because mobile devices in the network subject to change and create different paths dynamically among themselves to broadcast packets. Every sending node functions as a router to forward packets if it is not an ending node. MANET can be depicted as a random graph because the devices in the wireless network keep on moving. MANETs has dynamic topology it possesses several salient features like resource constraints, limited physical security, and no infrastructure [1]. Due to decentralized nature of wireless networks, network intrusion is relatively easy. There are many security attacks that are faced by wireless ad hoc networks which are black hole attack, wormhole attack, rushing attack, message bombing, denial of services (DOS)/DDOS etc [2, 3, 4]. MANETs exhibit some of the characteristics to accomplish consistent and secure wireless communication. They may include confidentiality, availability, authentication, integrity and non-repudiation [5].

i. Confidentiality: Protection of sending data packets from malicious nodes. Intermediate nodes may eavesdrop the packet which is passing through those nodes
ii. Availability: Denying a service when it is required is one kind of attack happens in MANETs.
iii. Authentication: It is another security attack in MANET's environment. An attacker may imitate a node and achieve unauthorized access to resource and sensitive data when there is no string authentication.
iv. Integrity: Another security attack is integrity. It is giving assurance that information being received is changed or not.
v. Non-repudiation: It ensures that both nodes can never deny about their sending and receiving of information.

In [6,7] many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security.

2. Network Attacks in MANETs

Due to malicious node there are different types of attacks can be possible in MANETs which are discussed in this section.

i. A malicious node transmits false route updates because to that route failures occur frequently and therefore network performance degrades.
ii. A malicious node captures a packet and decreases its time-to-live and hence it gets dropped before its destination.

iii. A node can redirect the traffic by sending false route information which may lead to poor resource consumption and hence degraded network performance.
The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly [15].

MANETs attacks can be classified into two main categories.

2.1 Passive attacks

Passive attacks are those attacks that do not disturb network operations. Attackers snoop data exchanged in network without changing it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping [8].Detection of passive attack is difficult because the network operation itself does not get affected and altered.

2.2 Active attacks

Active attacks are performed by the malicious nodes. Active attacks involve some modification of data bits or creation of false stream of bits. Active attacks can be divided into internal or external category.

i. External attacks are carried out by malicious nodes that do not belong to the network.
ii. Internal attacks are formed by compromising nodes that are part of the network. In this attack malicious node gain unauthorized access.

Internal attacks are more severe and difficult to detect than external attacks. Active attacks carried out by an external node or an internal compromised node involves actions i.e masquerading or spoofing, alteration, fabrication and replication.

Table 1: Attacks classifications

Active Attacks	***Passive Attacks***
Data integrity, sniffing, spoofing, DOS and Man in the middle attack	Monitoring, traffic Analysis, footprinting,trashing

Here we are discussing some major active attacks.

2.2.1 Black hole Attack

Attacker announces a zero metric for all other destinations causing all nodes around it to route packets towards it. The malicious node broadcast fake routing information that claiming it has an optimum route and causes all other nodes to route packets through the malicious one and finally malicious node drops all packets that it receive instead of forwarding.

2.2.2 Wormhole Attack

Malicious node receives data packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

2.2.3 Replay attack

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8].

2.2.4 Byzantine attack

A compromised intermediate node or set of compromised intermediate nodes works together to carry out attacks e.g creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in degradation of the routing services [9].

2.2.5 Location disclosure attack

Attacker collects the node location information i.e route information and then plans for further attack scenarios.

2.2.6 Flooding

In this attack malicious node injects false packets into the network or creates ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way.

2.2.7 Spoofing Attack

In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.

2.2.8 Man- in- the- middle attack

A malicious node sites between the source and destination and then sniffs any information being sent between two nodes.

2.2.9 Denial of service

Here an attacker tries to block the specific network service or network operation

2.2.10 Jamming

In this attack, malicious node determines frequency at which destination node is receiving signal. And then it transmit signal on that the same frequency.

3. Cryptography in MANETs

In this section we are discussing some cryptography techniques to secure MANETs.

3.1 Symmetric cryptography

In this method both mobile nodes will share a single secret key to accomplish their communication securely. Let consider sending and receiving nodes are represented by s by r and secret key is represented by Sec_k

Sending node: Cipher format=E(Sec_k (datapacket))

Receiving node: D (Sec_k (cipher format))

The encryption key is closely related to the decryption key and in that they are identical. In cryptography, keys represent a shared secret between two or more nodes that can be used to achieve secure communication. The secret key can be obtained from trusted third party.

3.2 Nonce

In a mobile adhoc network, the cryptography term nonce (timestamp/random number) can be used to make data packets secure and to prevent a replay attack. The session key between two nodes is often generated from a random number and in the public key mechanism the shared secret key can be generated from a random number.

3.3 Public/Private

It is also known as asymmetric cryptography. In this technique, there is a pair of public/private keys. The private key is kept private and the public key can be globally known to others. RSA [10] is the one of the earliest public-key cryptographic techniques and was developed by Ron Rivest, Adi Shamir, and Len Adleman.

If i, j are the sending and receiving mobile adhoc nodes then following cryptography notations can be used to achieve privacy between them

Cipher= E (PU_j ($Datapacket_i$))

Datapacket=D (PR_j (Cipher))

The success of PKI depends on the availability and the security of a Certificate Authority (CA), a central control point that everyone trusts[12].Certificate Authority will be a trusted third party with both nodes.

3.4 Certificate Issue Authority

In cryptography CA is an entity that issues a digital certificate to sending and receiving parties. In MANETs CA plays an important role to authenticate nodes during bootstrap stage. Digital certificate contains node id, issue time, expire time, public key, hash and encrypted using CA's private key.

4. Proposed Technique

As we know that there is no fixed infrastructure in adhoc network so security is a major issue. As MANETs typically lack a central authority for authentication and key distribution, security mechanisms must be scalable and capable of frequent topology changes [11]. The trust component is an important concept in network security, as it is the set of relations among agents participating in the network activities[13]. In this section we proposed cryptography based secure technique to handle malicious node in MANETs.

The technique consists of following steps.

i. There will be a dedicated node called registration node (RN) and its function will be to generate and assign registration tokens to each and every node.

ii. Whenever the two nodes want to communicate with each other they have to request to RN for a registration token.

iii. The request packet will contain source node identity,timestamp,home address and token request.
RP= (Nid,timestamp,h_add_{SN},req_R)

iv. When RN receives request from a source node, first it will check the node identity and its home address that to whom network it belongs.

v. After successful confirmation it generates a registration token and assign to node. Registration token will contain node ID,timestamp, duration, public key, nonce and that token will be encrypted using private key of RN.
RT=E (PR_{RN} (Nid,timestamp,duration,PU_{RN},N_A)

vi. After receiving the Registation token by a source node it sends an ACK signal to RN. The ACK signal will contain node ID,timestamp and nonce.The ACK signal will be encrypted using Public key of RN
ACK= E (PU_{RN} (Nid,timestamp,N_A)

vii. Steps iii-vi will be carried out between destination node and RN too.

viii. After getting registration token from RN by both source and destination nodes now they can proceed their communication.

In the above steps it is clearly mention that without getting registration token no commination can be initiated between nodes. Registration node will only assign tokens to valid and authentic nodes and this will be confirmed by registration node from the node identity and its home address in request packet.

Table 2: Notations used in proposed technique

Notations	***Abbreviations***
RN	Registration Node
Nid	Node identity
h_add_{SN}	Home address of Source node
RP	Request packet
PU_{RN}	Public key of registration node
ACK	Acknowledgement
req_R	Request of registration

5. Conclusion

MANETs is an adhoc and unsecure network. There is no

fixed infrastructure and static topology in MANETs. As the topology is dynamic so malicious node may be easily entered into MANETs environment and different attacks may be possible during nodes communication. This leaves MANETs open for a research. In this paper we have discussed MANETs active and passive attacks and proposed a technique based on node registration process using cryptography functions.

6. REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, pp. 38-47, 2004.

[2] Nagrath, Preeti, Gupta, Bhawna " The Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey". 3rd International Conference on Electronics Computer Technology (ICECT), 2011. Page(S): 245 – 250.

[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Attacks In Wireless Networks," *IEEE J. Selected Areas In Comm.,* Vol. 24, No. 2, Feb. 2006, Pp.370–380.

[4] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks And Defense In Wireless Ad Hoc Network Routing Protocol". Workshop On Wireless Security Proceedings Of The 2nd Acm Workshop On Wireless Security San Diego, Ca, Usa, 2006.

[5] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer, 2006.

[6] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[7] S. Kurosawa et al., "Detecting Blackhole Attack on AODVBased Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. N etwork Sec., 2006.

[8] Priyanka Goyal, Sahil Batra, Ajit Singh." A Literature Review of Security Attack in Mobile Ad-hoc Networks", International journal of Applications (0975-8887), Volume 9.No 12,November 2010.

[9] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. *Proceedings of the ACM Workshop on Wireless Security*, pp. 21-30, 2002.

[10] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Commun. of the ACM, 21:120-126, 1978.

[11] L. Zhou and Z. Haas, Securing Ad Hoc networks, *IEEE Network Magazine*, Nov. 1999.

[12] Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai, A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS.

[13] Dang-Quan Nguyen, Louise Lamont, Using Cryptography in Trust Computing for Networked Communications, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[14] D.-Q. Nguyen and L. Louise, "A New Cryptography Scheme for Selective Broadcasting." In proceedings of IEEE International Conference on Information and Computer Networks, ICICN 2011, Guiyang, China, 2011.

[15] Aishwarya Sagar Anand Ukey, Meenu Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010.

Rashid Jalal Qureshi is an Assistant Professor in Computer Science Department, Islamia College Peshawar (Chartered University). He received his PhD degree in Computer Science from Université François-Rabelais de Tours, Tours, France. He did Post-Doc from University of Debrecen, Debrecen, Hungary. He has several research papers in international conferences and reputed journals. His research area is computer graphics, image processing and visual cryptography**.**

Khalid Haseeb is a Lecturer in Computer Sciences Department, Islamia College Peshawar (Chartered University). He has done M.Sc in Computer Science from University of Peshawar, Pakistan. He did MS-IT from im|sciences Peshawar, Pakistan. He has 8 research papers in international conferences and journals. He has more than 8 years of experience in academics. He obtained international network certifications from Microsoft and Cisco. His research area is cryptography and network security.

Muhammad Arshad is an Assistant Professor in City University of Science and Information Technology Peshawar. He received his PhD degree in Computer Science from Liverpool John Moores University, Liverpool UK and he has more than 8 years of experience in research and academics. He did several research publications and his areas of expertise are Peer-to-Peer networks, network appliances, Quality of Service, Network Security, Web Services and Home Network.

Huma Javed has done her BSc and MSc in computer science from university of Peshawar in 1986-87 and 1990 respectively. She did her PhD from Liverpool John Moores university UK in 2009 in Middleware in WSN. She has been teaching in university of Peshawar for the last two decades and also has taught in UK. Her research interest in middleware, wireless sensor networks, embedded systems. She has published in many reputed international journals.

Haleem Farman is a Lecturer in Computer Science Department, Islamia College Peshawar (Chartered University). His research area is computer networks and MANETs**.** He is a PhD scholar in Computer Science Department University of Peshawar.