Prevention of Black Hole Attack in Secure Routing Protocol

Mayuri Gajera[1], Sowmya K. S[2]

Dayanand Sager College of Engineering, Bangalore, India

Abstract: ***Mobile Adhoc Network (MANET) consists of a collection of mobile nodes which do not require intervention of any existing infrastructure or centralized access point such as base station. MANET routing protocol are responsible for communication between mobile nodes. But MANET Routing Protocols are highly vulnerable to various attacks on layers of OSI model. Therefore security of routing protocol becomes must. This paper considers a secure routing protocol for Ad hoc on demand distance vector (AODV) routing protocol known as Identity-based key management (IKM) which is a combination of ID-based Cryptography and threshold cryptography and authenticates all routing message. Major concentration in this paper is on black hole attack. We attempt to show how black hole attack is prevented in IKM system. We use NS2 simulator to show the results for same.***

Keywords: AODV, IKM, Black hole, NS2.

1. Introduction

Mobile ad hoc networks (MANETs) are gaining attention in both the research and industry communities due to their characteristics of infrastructure less environment, no central control, and node mobility, self-organized. Due to such characteristics, they are susceptible to many types of attack [6] [18]. Wireless communication, for example, is open to interference and interception. The attacker might create, alter or replay routing message to disrupt the network operation. The attacker can harm the data in network by accessing it, or dropping data packets, or injecting bogus data in communication.

Several secure routing protocols are found for MANETs in literature [4] [8] [11] [12] [13] [14]. All these protocol uses key-setup problem where each node processes one or more key for itself and authenticate key information. Secure routing protocols in general authenticate all the routing messages in network. Most of the protocol uses trust model to authorize the node in a network whereas others uses digital signature to guarantee the integrity and authenticity in network.

Cryptographic mechanisms provide some of the strongest techniques against most vulnerability. Traditional cryptography system is divided into symmetric and asymmetric depending on the use of key. Traditional symmetric systems are difficult to apply in MANETs [5] as symmetric systems require less processing than asymmetric ones and they are not scalable as they demand that secret keys must be shared either by a secure pre-established channel or before network formation.

Several key management schemes are found for MANETs in literature [2] [3] [4] [7]. Key management deals with dynamic topology that is self-organized and decentralized in MANETs. It must satisfy requirement as:

- Not having a single point of failure.
- Compromise of certain number of nodes does not affect security between non-compromised nodes.
- Able to efficiently and securely revoke keys of compromised nodes and update keys of non-compromised nodes.
- Efficient in terms of storage, computation, and communication.

This paper deals on ID-based key Management (IKM) [14] which secures the AODV routing protocol [1]. We then show how Black hole attack is prevented in IKM. IKM is a certificateless approach where no central trust authority is required to certify or authorized the nodes in network.

2. Black Hole Attack

In black hole attack, a malicious node advertises itself for having the shortest path to the destination node. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the reply packet reaches the initiating node before the reply packet from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them like dropping the packet, retrieving information from packets or data packets are never reached to actual destination.

Figure.1 shows black hole attack where malicious node acts as intermediate node. here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ (route request) packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be consumed or lost.

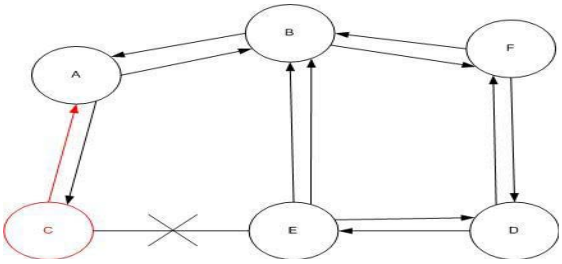

Figure 1: Malicious node as intermediate node

Figure.2 shows black hole attack in which malicious node "A" act as the destination node. "A" first detects the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP (route reply packet) which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

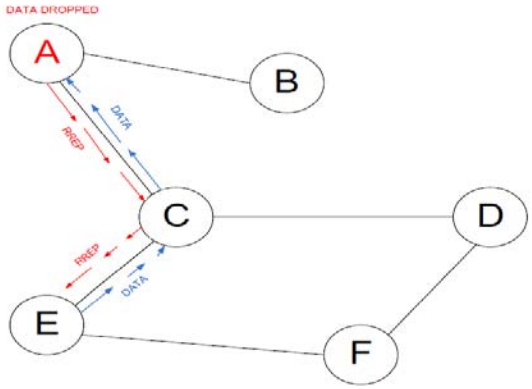

Figure 2: Malicious node as destination node

3. IKM

IKM [14] is a simple key management scheme where each node uses unique identity such as email-address or IP address to generate derive public and private key. In this paper we use IP address as a nodes unique identity. IKM adds some security parameter in the original AODV routing messages so as to authenticate the messages.

IKM is a combination of ID-based key management and threshold cryptography [10] [15]. In IKM the public and private key of each node are composed by a node-specific ID-based element and a network wide common element. The node-specific element ensures secrecy of non-compromised nodes in the presence of several compromised nodes. On the other hand, network-wide common element enables very efficient network-wide public and private key updates via a single broadcast message.

IKM consists of three phases: key predistribution, key revocation, and key update. The key predistribution occurs during network initialization which determines system parameters and preloads every node with appropriate keying material. It distributes its functionality to *t* distributed public key generator (PKG), called D-PKGs. The private master key is distributed using a threshold *t*-over-*n* cryptography. This is done to enable secure and robust key revocation and key update during network operation.

Key revocations must minimize the damage from compromised nodes. During network operation, if any node suspects that another node is malicious or has been compromised, it sends an accusation message to the DPKG. A node is considered bad when the number of accusations reaches a predefined value, called the revocation threshold against it. The identity of compromised node is stored in memory of each non-compromised node for some time period to stop communication with compromised node.

Nodes update their public/private keys in periodic intervals or when the number of compromised nodes reaches a predefined value. Compromised nodes cannot update their keys, thus becoming isolated from the network.

3.1 IKM with Black Hole Attack

The malicious node entering the network to interrupt the routing process in network cannot enter as they are unaware of the security parameter of the network. They are unable to change the RREP by changing the hop count or sequence number or spoofing the destination address of node as the RREP is authenticated and has no knowledge about the secure parameters. Hence is unable to unauthenticate the packet. Also if malicious node try to flood the network with bogus packets then such packets are dropped as they are not authenticated and if authenticated, still they are dropped as the secure parameters do not match.

4. Simulation Setup

We use NS2.34, a popular network simulator. We simulate MANET with 20 nodes deployed in 1500 x 1500 m^2 square fields. The MAC protocol used is IEEE 802.11. Frequent node mobility is not considered. The data is transferred at constant bit rate (CBR) with packet size of 1000 byte. We consider 4 D-PKGs and threshold value as 5. We simulate network performance by considering presence and absence of black hole node in network.

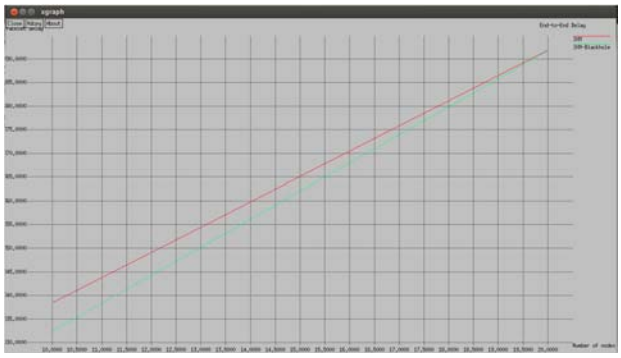

Figure 3: End-to-End Delay

End-to-End Delay: The average delay between the sending of the data packet by the CBR source and its reception by CBR receiver. It includes all the delays caused during route acquisition, buffering and processing at intermediate nodes,

and retransmission delays. Figure 3 shows the comparison between IKM and IKM with black hole, from which we say that the difference is almost negligible and hence black hole does not affect the delay of packets in network.

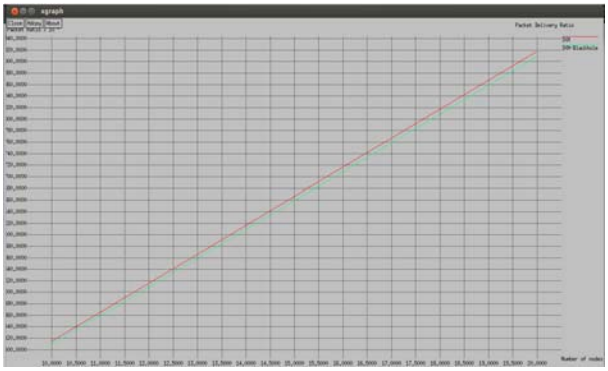

Figure 4: Packet Delivery Ratio

Packet Delivery Ratio: The data packets generated by the CBR sources that are delivered to the destination are evaluated by the ability of the protocol to discover routes. Figure 4 shows comparison between IKM and IKM with black hole, from which we say that the difference is almost negligible. Figure 4 shows the comparison between IKM and IKM with black hole, from which we say that the difference is almost negligible and hence black hole does not affect the delivery of packets in network.

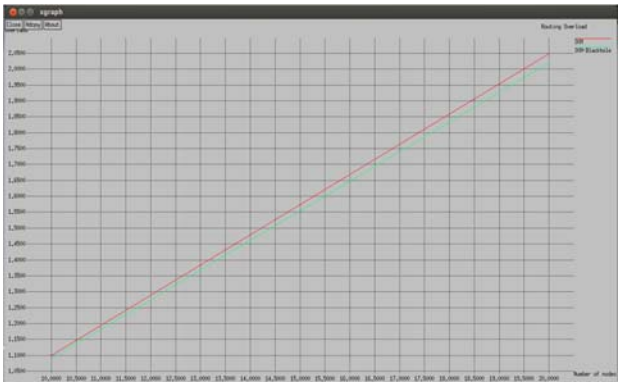

Figure 5: Normalized Routing Load

Normalized Routing Load: the packets are measured by average amount of routing packet transmitted per delivered data packet based on CBR packets. Figure 5 shows comparison between IKM and IKM with black hole, from which we say that the difference is almost negligible. Figure 4 shows the comparison between IKM and IKM with black hole, from which we say that the difference is almost negligible and hence black hole does not affect the routing load in network.

5. Conclusion

Security is a challenge in MANETs. The IKM system uses certificateless approach where each node derives its public key from its network ID and some common shared information. IKM is a secure, lightweight and scalable scheme for MANETs. The system identifies compromised node and prevents from third party attack which may also include trusted third party attack. We also show how the black hole is prevented in the IKM system. Thus we believe that IKM system is very secure system compared to other secure system when black hole attack, third party attack and compromised node is considered.

6. Future Scope

In IKM, the data packets are publicly seen which is vulnerable to attacks. Hence to protect the data packets we can encrypt/decrypt the packets using encryption/ decryption algorithm.

References

[1] Charles E.Perkins, Elizabeth M, Samir R.Das, tools.ieft.org/id/draft-ietf-manet-aodv-13.txt, "Ad-hoc On-Demand Routing Distance vector Routing Protocol", mobile ad-hoc working group, Internet Draft, 17th February, 2003.

[2] Yih-Chun HU, Adrian Perrig, "A survey of secure wireless ad hoc routing" In IEEE Security & Privacy, 2004.

[3] Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic, "Routing and Security in Mobile Ad-hoc network", IEEE Computer Society, Feb. 2004.

[4] Loay Abusalah, Ashfaq Khokhar, Mohsen Guizani, "A survey of secure Mobile Ad hoc routing Protocol" IEEE Communication Survey & Tutorials, Vol 10, No.4, 2008.

[5] I.Chlamtac, M. Conti, and J.J-N. Liu, "Mobile AdHoc Networking: Imperative and Challenges", AdHoc Networks, Vol. 1, no.1, pp. 13-64, 2003.

[6] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[7] Eduardo da silva, Aldri l. dos Santos, and Luiz Carlos p. albini, "ID-Based Key Management in Mobile Adhoc Networks: Techniques and Application", IEEE wireless communication, pp 46-52, October 2008.

[8] Davide Cerri and Alessandro Ghioni, Cefriel, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communications Magazine, February 2008.

[9] Dan Boneh, Matthew Franklin, "Identity-Based Encryption from the Weil Pairing", SIAM J. Computing, vol. 32, no. 3, pp. 586-615, Mar.2003.

[10] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," Proc. CRYPTO '89, pp. 307-315, Aug. 1989.

[11] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, "Authenticated Routing for Ad-Hoc networks", IEEE Journal on selected areas in communications, Vol.23, No. 3, March 2005.

[12] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Mobile Computing Systems and Applications, pp. 3–13, 2002.

[13] W. Liu and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," *Proc.* IEEE INFOCOM 2004.

[14] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, ”Securing Mobile Ad Hoc Networks with Certificateless Public Keys”, IEEE transactions on dependable and secure computing, vol. 3, no. 4, october-december 2006.
[15] A. Shamir, “How to Share a Secret,” Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.
[16] Akansha Saini, Harish Kumar “Effect of black hole attack on AODV routing protocol in MANET”, IJCST Vol. 1, Issue 2, December 2010.
[17] Jaspal Kumar, M. Kulkarni, Daya Gupta, “Effect of Black Hole Attack on MANET Routing Protocols”, I.J. Computer Network and Information Security, vol 5, pp 64-72, 2013.
[18] “Mobile Ad-Hoc Network”, www.olsr.org, www.it.iitb.ernet.in
[19] “Identity-Based encryption- An Overview”, www.iitg.ernet.in/cse/ISEA/isea_PPT/PalashSarkar.pdf
[20] NS2 tutorial, www.isi.edu/nsnam/ns/tutorial.

Author Profile

Mayuri Gajera is pursuing M.Tech degree in Computer Network from Dayananda college of Engineering from Visvesvaraya Technological University. She has 3 years of teaching experience. Her research area includes wireless network, Adhoc network, and network security.

Sowmya K S received B.E. degree in Computer Science and Engineering from SJMIT, Kuvempu University in 2001 and M.Tech from DSCE, VTU in 2008. Her research interest includes routing and security in WSN and MANETS. She is currently working as an Assistant Prof. at Dayananda Sagar College of engineering.