International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

A SECURITY BASED ARCHITECTURE FOR MANET

Ekata Gupta [1], Dr. S. K. Saxena [2]

[1] MCA Department, GNIM, New Delhi and Research Scholar, Mewar University

[2] CSE Department, Delhi Technological University (Formerly Delhi College of Engineering)

Abstract

A Mobile ad Hoc network is a kind of mobile network that is dynamically changing and they have a fully decentralized topology. The security of Mobile Ad hoc Network (MANET) is more rigorous than that of traditional network. Therefore security remains a major challenge for these networks due to their feature. Moreover in the absence of central monitoring points there is a lack of defense mechanism. An intermediate node which takes part in packet forwarding may behave differently and drop packets instead of forwarding them. This malicious node falsely advertises itself as a trustworthy node; such behavior is called black hole attack. In this paper security architecture for detecting a cooperative black hole attack is presented.

Keywords: MANET, AODV, security, cooperative Black hole.

I. Introduction

In the recent years, wireless technology has a tremendous rise in popularity and usage, thus opening new fields of applications in the domain of networking. One of the most important of these fields concerns mobile ad hoc networks (MANET), where the participating nodes do not rely on any existing network infrastructure. At any time and any place, the MANET can interlink

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

many mobile terminals in limited region .Therefore; the interconnections between nodes are capable of changing on continual and arbitrary basis.

Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. These include passive eavesdropping, active interfering, and denial- of service.One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols.

Our approach detects the packet forwarding Misbehavior detection and detection of routing misbehavior using AODV protocol.

AODV is vulnerable to the well-known black – hole attack although there has been lot of research on detection and prevention of an attack in MANET, most of the schemes have low detection rate, high complexity of detection algorithms, security vulnerabilities in the schemes themselves or high rate of false positives.

In this paper a mechanism is proposed to identify cooperative black hole with the help of security architecture design.

II. Security analysis of MANET

MANET is different from the fixed IP network as well as the general wireless network, which poses new challenges to guarantee its security The security threats confronted by MANET is the extension and expansion of that be confronted by wired network in the wireless field, which mainly comes from wireless channels and networks. The threats can be divided into two categories of passive attack and active attack.

1) Passive attack

Passive attack is essentially to listen or surveillance the message transmission process to obtain some secret

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

2) Active attack

Comparing with passive attack, the passive attack usually does not change the transmission data, while active attack will tamper data stream or create false data stream. The active attack includes four kinds of message replay, Fraud Counterfeiting, Message tampering and Denial of Service

III. Cooperative black hole attack

A malicious node that incorrectly sends, the RREP that is has the latest route with minimum hop count to destination and then it drops all the receiving packets, this is called black hole attack. Black hole attack in AODV can be performed in 2 ways

1. Using Route Reply(RREP)
2. Using Route Request(RREQ)

If multiple malicious node gather together to work cooperatively the attack effect is more This is known as cooperative black hole attack.

The black hole attack works in two phases. In the first phase the malicious node advertises itself of having a valid route to the destination even though the route is spurious. In the second phase the attacker node drops the intercepted packet without forwarding them. There is more subtle form of attack when the attacker suppresses or modifies the packets.

Now when these malicious nodes work in groups it becomes even more subtle.

IV. Cooperative Manet security architecture design

A. Objective of MANET Security

The objective of MANET security are in accordance with that of traditional network ,including data availability, confidentiality , integrity , security authentication and non-repudiation . Availability indicates that even in the face of various attacks normal services required are available.

Confidentiality means that unauthorized entities cannot access the information.

Integrity means that the information cannot be modified or destroyed Security

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

authentication indicate that both the ends are authenticated to send and receive message

Non-repudiation means sender cannot deny that message it has sent and similarly the receiver cannot deny that message has been received.

B. Security architecture of MANET

Security should develop together with the network as an integral part but not a remedial measure. Even though OSI layers provide us with the advantage of modularity, flexibility and standardization the security should be considered from layer to layer.

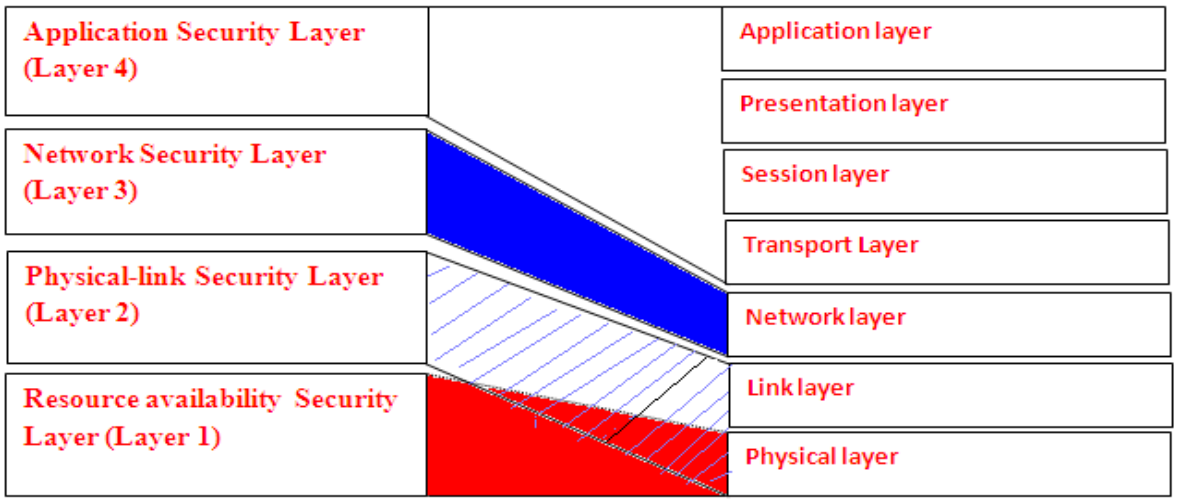

Fig 1: Cooperative Manet security architecture

According to the hierarchy idea of OSI model, the cooperative Manet security architecture is being designed.

1. Layer1 Resource availability security layer

This layer forms the foundation or the base of all the layers. The functions designed at

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

this layer would be used by the upper layers. Manet is an infrastructure less and distributed network so the security required for Manet should be of distributed kind .so with the help of this layer a security relationship can be established between the nodes.

2. Layer 2 Physical-link security layer

When we look at the wired or wireless network there is some kind of protection mechanism through firewall or through access control but in Manets the channel can be attacked from any direction and on any node. The main task of this layer is to protect the data from tampering or destroying.

3. Layer 3 network security layer

In Manet a node must play two roles (I) communication with other nodes (ii) routing of packets .In addition a host may be required to forward a meant packet. The former requires mutual cooperation and sharing correct routing information among the nodes to maintain the network connection in correct.

Routing is most important in Manet for it relates to the topology of the whole network this mechanism modifies the AODV protocol by introducing data routing information (DRI) table which each node maintains. Two additional bits are being sent along the RREQ message. This first bit indicates routing information from the node and the second bit indicates routing information through the node.

When a node as N1 generates a packet for node N2 the following task are performed

i. The ids of both the nodes are recorded.
ii. A record to keep track of number of receiving and forwarding packets to and from node N2.
iii. The entire record is signed by node N1 using its private key.

Each node also maintains a self table (ST) and a Recorded table (RT)

A. ARCHITECTURE:

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

In this architecture of cooperative security agents we pass DRI and ST-RT table as an input to Cooperative Security Agents. Monitor processing takes charge of monitoring all one-hop neighbors' activities and filtering and encoding them. In the Memory Library, the behavior patterns of attack nodes are kept to represent various known attack methods.

Mode 1: Rec (N1, M), Delete (N1, M). Node N1 receives the message M and then deletes it, not transmitting it in accordance with the routing table. It is Interrupt Attack.

Mode 2: Rec (N1, M), Modify(S N1, M), Send (N1, M). Node N1 receives the message M, and then transmitting it to next hop node after modifying packet content. Next hop node will receive the wrong packet information. It is the Error Message Attack.

Mode 3: Rec (N1, M), Reply (M, N), Send (N1, N). Node N1 receives message M, and then sends the reply message to make wrong routing direction. It is the Black Hole Attack.

Mode 4: Make (N1, M), Broadcast (N1, M). Node N1 generates and broadcasts a large number of messages in a short period of time, leading to normal nodes not working properly. It is DoS Attack.

If one behavior matches the previous defined attack patterns, it is likely to be attack node the role of the decision-making module is to identify attacks, position the invaders, and send out an instruction to its neighbor nodes to arouse the Counterattack Agents.

In addition to this the black hole detecting component is used to collect the network node ID of these nodes and to analyze them.

Thus it would reduce the time required for black hole detection about a particular node and improve the system performance.

In Alert, Responses and cooperative agent module is used to identify the alert level of the node.

1 Serious : Drop the node Id and alert all the neighboring nodes

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

2 Moderate : Dynamic decision is taken whether to drop the node or not

3 Slight: do not care condition.

The cooperative and communication agent is used to receive alert messages from other security agents. After receiving these alerts the agent makes a judgment is larger than 0.5 and then adds a new rule to its table

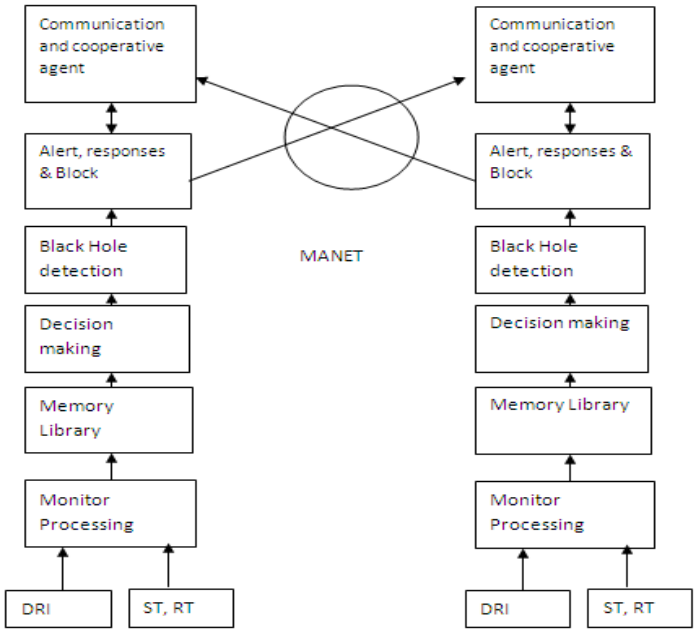

Fig 2: Architecture of Cooperative Security Agents

4 Layer 4 Application security layer

The application security layer refers to the security of End-system, such as security protocols of Secure Socket Layer (SSL), Secure Shell (SSH), Secure Electronic Transaction (SET) and others. The protocols are independent of the underlying network security layer, which encrypt the data before it enter into the network layer to ensure data

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

security. In the layer, the security protocol being used is determined by the application programs running in the system, such as SSL is the protocol to enhance security Web transmission; the SSH is the protocol to enhance security Telnet/FTP transmission.

The application security layer is corresponding to four layers from the transport layer to the application layer of OSI model, which defines secure mechanisms related to application programs in the end systems, such as SET protocol, so it is separated from the underlying layers.

V. Conclusion

Owing to characteristics of open medium, dynamic topology and distribution, the security of Mobile Ad hoc Network (MANET) is more rigorous than that of traditional network. Referring to the hierarchy idea of OSI reference model, the paper divided the security architecture into four layers of Layer1 Resource availability security layer, Layer 2 Physical-link security layer, Layer 3 network security layer, Layer 4 Application security layer.

The functions of each layer ware also described in detail. Thus, the security mechanism of the whole network is considered from the aspect of system architecture, which provides framework for secure network design.

A security method has been proposed to detect black hole and cooperative black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node by avoiding the black hole nodes.

This mechanism can effectively detect malicious nodes and mitigate the negative impact caused by the Black hole and cooperative black hole attack.

VI. References

[1] Sen, J.; Koilakonda, S.; Ukil, A., "A Mechanism for Detecting of Cooperative Black hole Attack in Mobile Ad Hoc Networks", Second International Conference on Intelligent Systems, Modelling and

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 4 Issue 1 January 2014

International Manuscript ID : 2249054XV4I1012014-01

Simulation (ISMS), pp.338-343, Jan. 2011.

[2] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008.

[3] Abderrahmane Baadache, Ali Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[4] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng "Research on MANET Security Architecture Design" , 2010 International Conference on Signal Acquisition and Processing

[5] Vaishali Mohite, Lata Ragha "Cooperative Security agents for Manet" , 2012 World Congress on Information and Communication Technologies

[6] Mishra A., Nadkarni K. and Patcha A., "Intrusion Detection in Wireless Ad hoc Networks," IEEE Wireless Communications, vol.11, 2004, pp. 275-283.

[7] Xia Ye, Junshan Li," A Security Architecture Based on Immune Agents for MANET" ICWCSC 2010X

[8] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom' 2000, pp. 275-283.

[9] Azer, M.A., et al., A Survey on Trust and reputation Schemes in Ad Hoc Networks, 3rd Intl. Conf. on Availability, Reliability and Security (ARES), 2008.

[10] Omar, M., Challal, Y., and Bouabdallah, A., Reliable and Fully Distributed Trust Model for Mobile Ad Hoc Networks. Computers & Security, 2009.Vol. 28 No.(3-4): p. 199-214.