International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Security in Wireless Ad-hoc Network

Shahuraj Patil[1], Jyoti Raghatwan[2]

[1]Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2]Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

Abstract: ***A wireless ad hoc network is a self-configuring network that is formed automatically by a collection of mobile nodes. In the wireless ad hoc network there is no centralized management. The malicious nodes can access the network, so there are many possible attacks in wireless ad hoc network. In the wireless adhoc network there a is high security risk. The adhoc networks are vulnerable to Dos attacks on the network layer. Black hole, Gray hole and worm hole attacks are the widespread attacks on adhoc networks. In a black hole attack the malicious node attracts traffic towards it and drops all packets without forwarding to the target or destination. The security of the AODV (Adhoc On-demand Distance Vector) protocol is compromised by a particular type of attack called black hole attack.. The malicious nodes disturb the data transmission in the network by transmitting false routing information. In this paper we are going to present an efficient Adhoc On-demand Distance Vector (AODV) protocol that removes the malicious node by isolating it and ensure the safe communication. In wireless adhoc network the new nodes can join or leave at any time. So, an efficient security mechanism is needed to detect malicious node .So, these nodes are to be arranged in spanning tree fashion. RSA key exchange and two encryption techniques are used among authenticated neighbors in the adhoc network to provide more security and thus avoid group rekeying problems.***

Keywords: Adhoc network, AODV, Gray hole attack, Black hole attack, RSA key exchange

1. Introduction

Ad-hoc network is defined as a category of wireless networks that utilizes multi-hop radio relaying and is able to operate without the support of any fixed infrastructure. Nodes communicate directly to one another over wireless channels. The routing and resource management are in a distributed manner, such that all nodes co-ordinate to enable communicating between them. Ad hoc network is self configuring, self- maintence and quick and easy to utilize network in any situation. The mobile nodes within the network can be moving or fixed position objects equipped with antennas they can either human moving in mall or network use unlicensed frequency spectrum due to these characteristics of wireless ad-hoc network, these network can be used in uncertain situation like flood, disaster, education, monitoring etc. The ad-hoc network is used to share information. Main benefit of wireless ad-hoc network is dynamically changing topology, absence of infrastructure such that mobile ad-hoc network changes continually and nodes can continually move into and out of radio range of other nodes. Ad-hoc network enables wireless device to communicate with one another as needed even when there is access to the internet is unavailable. Wireless communication is possible without routers, base station or internet service provided. Key application of wireless ad-hoc network are conforcing, home networking, emergency services Bluetooth etc. Nodes having mobility, communicate via radio broadcast medium, so used in military communication by soldiers. The characteristics of wireless ad-hoc network along with mobility and broadcast medium leads to some major issues for wireless ad-hoc network such as ip addressing ,radio interference ,routing protocols, power constrains, security ,mobility management etc . Among all research issue, though one of obligatory research issue in wireless ad-hoc network is security.

Security is difficult to be achieved in wireless ad-hoc networks because of vulnerability of links, the limited physical protection of each of the nodes, dynamic changing topology, and absence of a certification authority and lack of a centralized monitoring. Recent history of Internet and of cellular network has shown that if security of a given network architecture is not properly designed from the very beginning and then security breaches will be exploited by malicious users. It is easier for hackers to eavesdrop and gain access to confidential information. It is easier for them to enter or leave a wireless network because no physical connection is required. Wireless ad-hoc networks have far more vulnerabilities than the traditional wired networks.

In this paper we developed an efficient security mechanism to secure group communication and by using AODV protocol we prevent Black hole and gray hole attack. In this mechanism, when the network consisting of multiple nodes is created, it first checks whether there is any malicious nodes existing in the network. To remove these malicious nodes, an advanced AODV protocol mechanism is used. Thus the malicious nodes are isolated. If any intermediate node receives false routing information from its neighbor node, then that node is to be considered as a malicious node. The intermediate node informs the other nodes about the malicious node through the route reply packet and every node getting the information updates its routing table to mark the node as a malicious. When a RREQ is sent, a list of malicious nodes is appended and the other nodes update its routing table. Thus, the nodes can identify the list of malicious nodes by identifying incorrect routing information or by checking routing table so that they can inform other nodes not to consider the routing information from the malicious nodes.

2. Literature Survey

A lot of papers were studied and following were shortlisted for careful analysis.

The paper titled "Survey of Mobile Ad Hoc Network Attack" by Pradip M. Jawandhiya, Mangesh M. Ghongep[5]

This article focus on all the existing attacks on MANETs. The author also describes the major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. The author provides us a brief comparison on attack types. In this survey paper, author try to find out the security threats in the wireless ad-hoc networks, which may be a main problem to the operation of it. Due to nature of mobility of nodes and open media MANET are much more vulnerable to all kind of security risks as covered. As a result, the need of security in the MANET are much higher than those in the traditional wired networks.

The paper titled "Prevention **and Detection of a Black Hole Attack in AODV based Mobile Ad-hoc Networks" by Nisha John, A Thomas[3]**

This paper has organize various works related to black hole attack detection methods in AODV-based MANETs and try to find out their advantages and disadvantages and at the end, the author compared these methods from some featuers and observe that the mechanisms detects black hole node, but no one is secure procedure since most of the solutions are having more time delay, more network overhead because of lately introduced packets and some mathematical calculations.

The paper titled "Secure Key Exchange and Encryption Mechanism for Ad Hoc Networks" by Sumathy, B.Kumar[2]

In this paper the Author propose novel security scheme in ad hoc networks is presented which can address the security problems such as authentication, confidentiality and key management that would avoid global re-keying. The author proposes a scheme which aims at sender deniable encryption can be widely applicable for voting and auction protocols. This shall be useful wherever group communications is to be established in a secured manner in an ad hoc environment.

The paper titled "A survey of black hole attacks in wireless mobile ad hoc networks," by Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao[3]

In this paper the author observe that both of proactive routing and reactive routing have specialized skills. In Proactive (table Driven) routing protocols the node in the network maintains routing information to every other node in the network. Routes information is kept in the routing tables and is periodically updated as the network topology changes. Reactive (On-Demand) routing protocol do not maintain routing information.

The paper titled "Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks, "by S. Sibichen [1]

In this paper the author apply the advanced version of AODV.And this AODV protocol is applied first to remove the malicious nodes causing Gray hole and Black hole attack. After detecting and removing malicious nodes are arranged in a spanning tree topology. Once the network is created, communication occurs only among the authenticated neighbors. In next step the RSA key exchange is applied before encryption and decryption of messages. To improve security, encryption has been done two times. It ensures the forward and backward secrecy. Whenever the topology change, the new neighborhood key is calculated and is given to all authenticated neighbors.

3. Methodology

An efficient security mechanism is developed to secure the communication between the nodes and to prevent Gray hole and Black hole attacks using AODV protocol. In this mechanism, when the network consisting of multiple nodes is created, it first checks whether there is any malicious nodes existing in the network. To remove these malicious nodes, an advanced AODV protocol mechanism is used. Then we construct a spanning tree that calculating the minimum distance between each and every nodes which can cover all the nodes without forming a cycle. We select the route with minimum distance. For security we use the RSA key exchange mechanism.

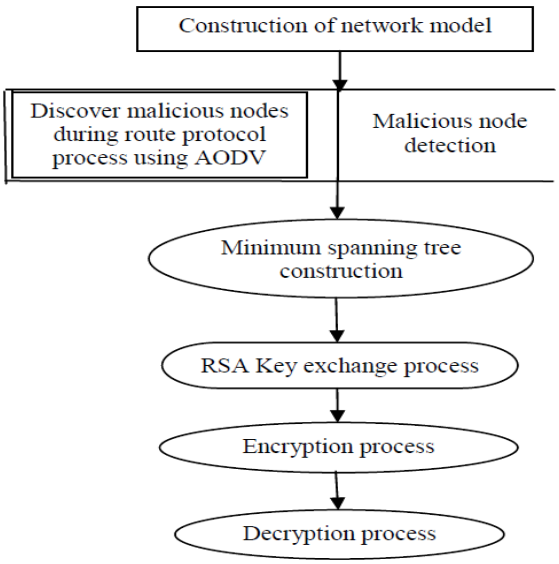

Figure 1: Proposed scheme architecture.

3.1 AODV Routing Protocol

AODV is a reactive routing protocol. A reactive routing protocol means it creates a route from source to destination only on demand. To find the route this routing protocol uses a reactive approach. In this protocol we use four message set: Route Request (RREQ), Route reply (RREP), Route Error (RERR), for link status monitoring (Hello).

The process of discovering route is started whenever a source node wants to communicate with another node. The Sequence number and broadcast ID is associated with the every node. If any intermediate node receives false routing

information from its neighbor then that node considered as malicious node. That intermediate node will inform to other node about that malicious node. After getting information about malicious node then every node will update its routing table to mark the node as malicious.

The nodes can identify the list of malicious node by identifying incorrect routing information or by checking routing table which was updated when malicious node found. When the node receives a route reply packet (RREP),it checkes the sequence number from the routing table. If the sequence number is greater than the one in RREP,the RREP packet is accepted; otherwise it will discarded.

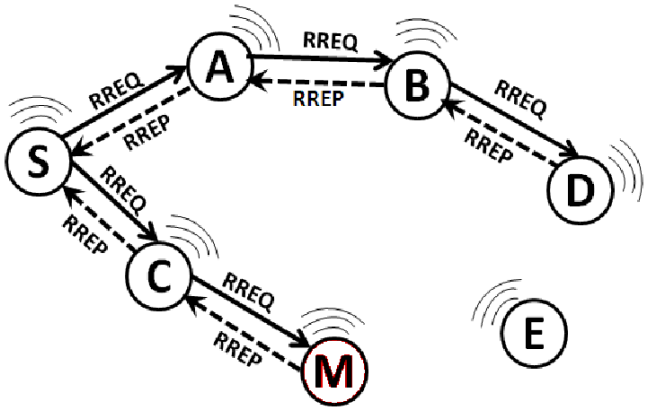

Figure 3.2: Route discovery protocol in AODV

The route discovery process in AODV in the presence of a malicious node M and a source node S broadcast route request packet(RREQ);the nodes within communication range, A and C receive the RREQ and again that re-broadcast RREQ to their neighbor until a node having a proper route or a valid route to the distination.The destination D receives RREQ and it will send RREP to source node on the reverse path of RREQ.The malicious node which present in the route sends RREP with higher, but fabricated, sequence number to the source; another RREP is sent by destination node D having genuinely higher sequence number to the source. As malicious node sends RREP with higher sequence number than the normal nodes sequence numbers chooses path through M to transfer data packet and therefore the malicious node can drop packets. An intermediate node dynamically calculates a PEAK value after every time interval that uses three parameter for calculation: RREP sequence number, routing table sequence number of replies received during the time interval.The PEAK value is the maximum possible value of sequence number that any RREP can have in the current state The RREP received from malicious node is marked as DO NOT CONSIDER.

3.2 Spanning tree construction

A spanning tree is calculating the minimum distance between each and every node which can cover all the nodes without forming a cycle. Spanning tree holds security tie-ups only with neighbor. Spanning Tree Protocol is a network protocol which establishes and maintains the spanning tree connecting a group of mobile node in the wireless ad hoc network.[1]

The distance between each node in the network is calculated by using the formula:

$$Distance(i,j)=\sqrt{(xj-xi)^2+(yj-yi)^2}$$

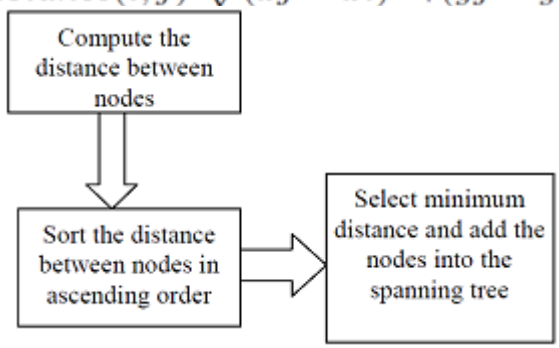

Figure 3.3: construction of spanning tree

3.3 Key Exchange mechanism

RSA key exchange mechanism is used to ensure security. Each and every node from the mobile ad-hoc network has its own symmetric key called the Neighborhood Key. For encryption and decryption each node must have access to the other node's neighborhood key[1].

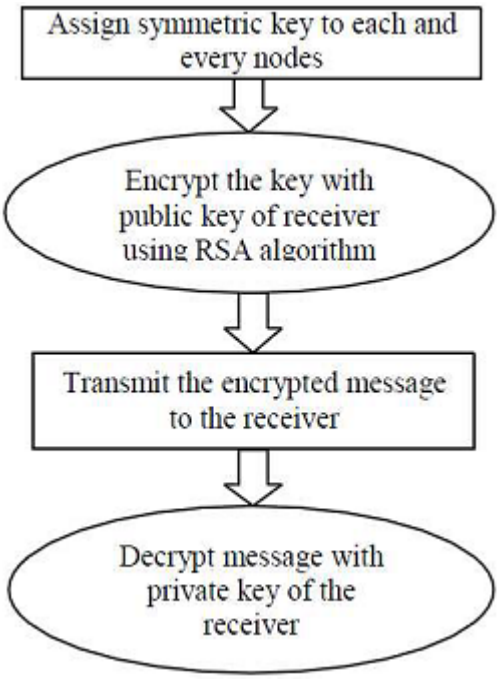

Figure 3.4: RSA key exchange

Encryption of Message: Every node has a symmetric key called neighborhood key. The message is first encrypted with the message specific key. Then, the message specific key is encrypted with neighborhood key .then sender appends the destination nodes ID and sends to its authenticated neighbors.

Decryption of Message: At the receiver, it first checks whether the ID matches or not. If the appended ID matches with the nodes ID, then it is the intended recipient and decryption is first performed with neighborhood key of sending node and the plain text message is obtained. Further decryption is done with the message specific key and the original message is obtained. If the ID does not match, that

node is not the intended recipient. So it re-encrypts the message with the neighborhood key and sends to its authenticated neighbor nodes. The procedure is repeated again until destination node is found and the original message is decrypted at the destination node [1].

4. Conclusion

A Mobile Ad hoc Network has open media nature and free mobility that's why it needs much more prone with respect to security risks e.g. intrusions, information disclosure and denial of service etc. A Mobile Ad hoc Network needs high level of security as compare to the traditional wired networks Security issues have overlooked while designing routing protocols for ad-hoc networks. Through AODV protocol, it is easier to breach the security of a wireless ad-hoc network. AODV is susceptible to many Do's attacks including Grayhole and Black hole attacks. Efficiently finds short and secure route to the destination.

5. Future Work

Wireless ad-hoc network required high level security. There is need to develop efficient security mechanism for avoiding different types of attacks. Planning to design more efficient routing protocol detect these attacks and to isolate the attackers so as to let the network perform in an attack free environment. So that study and implement secure network method, routing protocol for secure wireless ad-hoc network.

References

[1] An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks Sisily Sibichen1, Sreela Sreedhar2/(ICMiCR-2013).
[2] Secure Key Exchange and Encryption Mechanism for Ad Hoc Networks S. Sumathy/2009 First International Conference on Networks & Communications.
[3] A survey of black hole attacks in wireless mobile ad hoc networks, by Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao/Human-centric Computing and Information Sciences 2011
[4] Prevention and Detection of a Black Hole Attack in AODV based Mobile Ad-hoc Networks by Nisha John, A Thomas.
[5] Survey of Mobile Ad Hoc Network Attack by PRADIP M. JAWANDHIYA, MANGESH M. GHONGE.

Author Profile

Prof. Jyoti Raghatwan received the B.E. Degrees in Computer Engineering from Pune University, Pune. She is working as Assistant Professor in department of Computer Engineering, RMD Sinhgad School of Engineering Pune, India. She is having more than six year experience. Her research interest is in Information security.

Shahuraj Patil Reseach Scholar RMD Sinhgad of Engineering, University of Pune. He has received B.E. in Copmputer Engineering from Mumbai University, Mumbai. Currently he is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Pune, Savitribai Phule, Pune University, Pune.