IJCSC 0973-7391 Volume 6 • Number 1 Sep - Mar 2015 pp.94-99 available online at www.csjournalss.com

Survey of Secure Routing Protocols over MANET

Mani Goyal[1], Dr. Sunil Taneja[2], Sandeep Kumar[3]
[1,3]Department of Computer Science, Ganpati Institute of Technology & Management, Yamunanagar, India
[2]Department of Computer Science, Government College, Chhachhrauli, Yamunanagar, India
er.mani.goyal@gmail.com, suniltaneja.iitd@gmail.com, sandeep167@gmail.com

Abstract: In MANET each mobile node can directly communicate with other mobile node if both mobile nodes are within transmission range. Otherwise the nodes present in between have to forward the packets for them on network. In such condition each mobile node acts as a router to forward the packets for others. Forwarding packet in MANET with limited resources (like bandwidth constraints, hidden terminal and limited battery power) is a very challenging task. Till data may routing protocols were proposed are an improvement over a number of different strategies considered in the literature for a given network. So it is quite difficult to find out which protocol may perform better under different network conditions of MANET. In this survey paper we proved an overview of various routing protocols proposed by various researchers. We will also provide comparative study of some routing protocol to find out the performance of protocol for large MANET.
Keywords: Broadcast Hybrid, Inherent, Mobility, Multicast, Network, Security, Vulnerabilities.

I. INTRODUCTION

Mobile Ad-hoc Network is a collection of wireless mobile nodes dynamically forming a network without the use of any existing network infra-structure. The mobile hosts are not bound to any centralized control like base stations or mobile switching centres. Although this offers unrestricted mobility and connectivity to the users, the onus of network management is now entirely on the nodes that forms the network. A mobile ad hoc network is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols. Ad-hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed. 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. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. Nonetheless, these solutions are not always be suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. One of the very distinct characteristics of MANETs is that all participating nodes have to be involved in the routing process. Traditional routing protocols designed for infrastructure networks cannot be applied in ad hoc networks, thus ad hoc routing protocols were designed to satisfy the needs of infrastructure less networks. Due to the different characteristics of wired and wireless media the task of providing seamless environments for wired and wireless networks is very complicated. One of the major factors is that the wireless medium is inherently less secure than their wired counterpart. Most traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. This problem is enlarged in ad hoc networks since routing usually needs to rely on the trustworthiness of all nodes that are participating in the routing process. An additional difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks.

II. NETWORK SECURITY

Network security measures are needed to protect data during their transmission. To assess the security needs effectively and to evaluate and choose various security policies, we need a systematic way of defining the

requirements for security and characterizing the approaches to satisfying those requirements. Our approach is to consider two aspects of security:

- Security service: A service that enhances the security of the data processing systems and the information transfers. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
- Security attack: Any action that compromises the security of information owned by an organization.

A. Security Services

The classification of security services is as follows

1. Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying and other forms of disclosure, including simply revealing the existence of an object.
2. Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. Integrity: Ensures that only authorized parties are able to modify transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted information.
4. Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. Availability: Requires that computer system assets be available to authorized parties when needed.

B. Security Attacks

The nature of attacks varies greatly from one set of circumstances to another. In general, there is flow of information from a source to a destination. We have listed below the generic types of attack that might be encountered. They have also been pictorially depicted.

- *Interruption:* An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.
- *Interception:* An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network and the illicit copying of files or programs.
- *Modification:* An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.
- *Fabrication:* An unauthorized party inserts counterfeit objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

These security threats have been shown in figure 1.

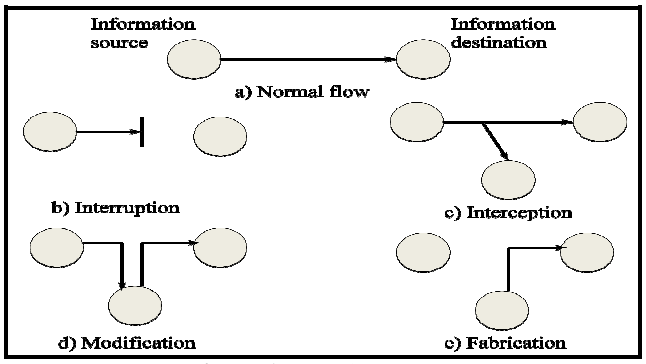

Figure 1: Security Threats

A. **Passive attacks**

An attack in which an unauthorized party gains access to an asset and does not modify its contents is called as passive attack. The passive attacker does not send messages; it only eavesdrops on the network as shown in figure 2. These attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted Two types of passive attacks are:

1. *Release of Message Contents:* The transmission may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of the transmission.

2. *Traffic Analysis:* This is a more subtle attack. Sometimes, even if the contents of the message are masked by using encryption techniques, the opponent might still be able to observe the pattern of messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data. However it is feasible to prevent the success of these attack. Thus passive attacks are prevented and not detected.

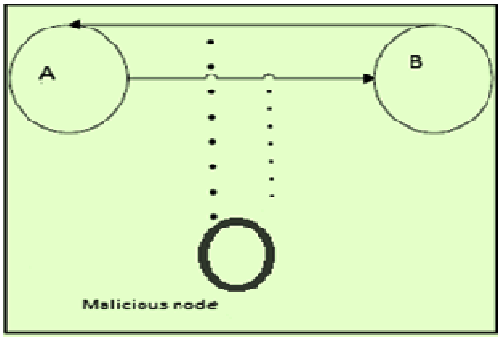

Figure 2: Active Attacks

B. **Active Attacks**

An attack whereby an unauthorized party makes modifications to a message, data stream or file is called as an active attack as shown in figure 3. These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.

1. Masquerade: This takes place one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attacks.
2. Replay: This involves passive capture of data units and its subsequent retransmission to produce an unauthorized effect.
3. Modification of Messages: This simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered.
4. Denial of Service: This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. Because the detection has a deterrent effect, it may also contribute to prevention.
5.

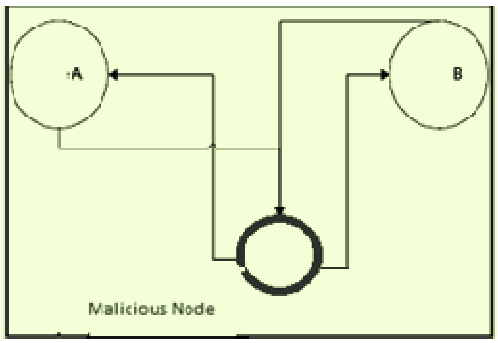

Figure 3: Active Attacks

We need to address security services in order to prevent the security attacks. However ad hoc network routing protocols do not need confidentiality as intermediate nodes process routing messages before forwarding in the network. The security mechanism based on cryptography is useful for preventing external attacks.

III. Secure Routing Protocols

1. SEAD [12]

Hu, Johnson and Perrig proposed secure efficient ad hoc distance vector (SEAD) [12] protocol that is based on the design of DSDV. SEAD is designed to prevent attacks such as DoS and resource consumption attacks. SEAD uses one way hash function for authenticating the updates that are received from malicious nodes and non-malicious nodes. This protocol is very efficient and can be easily implemented. However the protocol is robust against multiple uncoordinated attacks but is not able to prevent the attackers from broadcasting the routing message having same metric and sequence number which were used by the recent update message.

2. Ariadne [7, 11]

It is based on basic operation of DSR. Ariadne is a secure on-demand routing protocol and uses only high efficient symmetric cryptographic operations. Ariadne provides security against one compromised node and also prevents many types of denial-of-service attacks. Ariadne uses message authentication code (MAC) and secret key shared between two parties to ensures point-to-point authentication of a routing message. However, it relies on the TESLA broadcast authentication protocol for secure authentication of a routing message which requires loose time synchronization.

3. SAR [15]

Security Aware Routing is an on demand routing protocol based on AODV [3]. SAR defines level of trust as a metric for routing. Nodes distribute key with those nodes having equal level of trust or higher level of trust. Thus an encrypted packet can be decrypted only by the nodes of the same or higher levels of trust. The main drawback of SAR is that during the path discovery process, encryption and decryption is done at each hop which increases the power consumption. The protocol also requires different keys for different level of security which leads to increase in number of keys required when the number of security levels used increases.

4.ARAN [14]

K. Sanzgiri et al developed authenticated routing for ad hoc networks (ARAN), which is based on AODV. In ARAN, each node has a certificate signed by a trusted server whose public key is known to all legal nodes in the network. The ARAN ensures secure route establishment by end-to-end route authentication process. ARAN provides authentication, non repudiation and message integrity but needs a small amount of prior security coordination among nodes. The keys are generated a priory and distributed to all the nodes by the server. The ARAN prevents unauthorized participation, message modification attacks but prone to replay attacks if nodes do not have time synchronization. The ARAN uses asymmetric cryptography computation which causes higher cost for route discovery.

5. SAODV [13]

Zapata and Asokan proposed another protocol designed to secure AODV. The idea behind SAODV is to use a digital signature to authenticate the non-mutable fields of messages and hash chains to secure the hop count information. The SAODV described two methods to secure routing: Single Signature Extension and Double Signature Extension. When a node receives any message such as RREQ or RREP, it first verifies the signature before creating or updating a reverse route to that host. The SAODV is based on asymmetric key cryptographic operation therefore the nodes in MANET are unable to verify the digital signatures quickly enough as they have limited battery life as well as processing power. Moreover if a malicious node floods messages with invalid signatures then verification can be very expensive. The key features of all these protocols have been summarized below in table 1:-

Table 1: Features of Secure Routing Protocols

Name of the Protocol	Features
SEAD	➢ Uses one way hash function. ➢ Attacker cannot generate any value in hash chain. ➢ Very efficient mechanism.
ARIADNE	➢ Uses highly efficient symmetric key cryptography ➢ No guard against passive attackers. ➢ Does not prevent insertion of malicious data packets. ➢ Vulnerable to other attackers form broken link.
SAR	➢ Classifies nodes into different immutable trust levels. ➢ Can be implemented by distributing keys for each trust level. ➢ Not very scalable. ➢ Lot of computational efforts required.
ARAN	➢ Assumes managed-open environment. ➢ First stage is certification and end-to-end authentication stage. Source takes a trusted certificate from trusted server, signs the request packet. Each intermediate node signs the request with its certificate. ➢ Computationally expensive.
SAODV	➢ Implementation on AODV. ➢ Checks external attacks. ➢ Uses Key cryptography and hashing both. ➢ High overhead.

IV. ANALYSIS AND REVIEW OF LITERATURE OF SECURE ROUTING PROTOCOLS:-

Security in ad hoc network is big challenge. Still there are a lot of security threats to ad hoc networks. One of them is distributed denial of service attacks. The ad hoc networks are more vulnerable to the security attacks because they are infrastructure less and they don't have any centralized controlling authorities. There are no effective defence mechanisms against many important attacks and no guidance on how to select defence mechanisms. Existing defence mechanisms have been evaluated according to very limited criteria. Often relevant risks have been ignored or evaluations have been carried out under ideal conditions. Still a lot of work is to be done to prevent distributed denial of service attacks and finally to make ad hoc networks fully reliable and secure. The performance analysis of secure routing protocols has been given in table 2.

Protocol	**SEAD**	**ARIADNE**	**SAR**	**ARAN**	**SAODV**
Type	Proactive	Reactive	Reactive	Reactive	Reactive
Encryption algorithm	Symmetric	Symmetric	Asymmetric /Symmetric	Asymmetric	Asymmetric
MANET Protocol	DSDV	DSR	AODV	AODV/DSR	AODV
Synchronization	Yes	Yes	No	No	No
Central Trust Authority	Certification Authority Required	Key Distribution Center(KDC)Required	CA /KDC Required	CA Required	CA Required
Authentication	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	No	Yes	Yes	No
Integrity	No	Yes	Yes	Yes	Yes
Non Repudiation	No	No	Yes	Yes	Yes
Anti Spoofing	No	Yes	Yes	Yes	Yes
DOS Attacks	Yes	Yes	No	No	No

Table 2: Performance Analysis of Secure Routing Protocols

V. CONCLUSION

The routing protocols proposed for Mobile Ad hoc networks seem to meet the basic requirements like dynamically changing network topologies rather well. However, the security issues have been left primarily ignored. The MANET routing protocols must be secured from the viewpoint of the authentication, integrity and privacy. These requirements can be at least partially met by using strong authentication and encryption mechanisms, digital signatures, hashing and MACs. Moreover, the protection means can be optimized for every protocol based on the approach taken to routing. Some MANET routing protocol developers suggest the application of IPSEC within the protocol to achieve the necessary security goals. This kind of approach is not totally adequate, due to the problems of replay etc. Moreover, the traditional security mechanisms such as link-level encryption or bi-directional tunnels are not adequate, due to the dynamic and unpredictable nature of MANET networks. The proposed security algorithm is for detection of malicious nodes present in the network. The proposed approach presented a scheme to proactively prevent external attacks. The solution is specifically targeted for AODV protocol. which shows that the effect of the overheads caused by our scheme is marginal and has negligible effects on network performance.

VI. FUTURE WORK

It was found that not one method can carried out to make MANET routing secured. Many combinations were tried and it was found that each protocol behaves differently in each proposed plan. New scheme is incorporated on AODV because most of the work has been carried out using AODV as a base protocol. Proposed Scheme is compared with existing AODV without malicious nodes, with malicious nodes and results are analyzed based on the proposed approach. It was found malicious nodes are big issue in MANET routing. These malicious nodes drop the packets by using fake routes and it is very difficult to identify a malicious node.

We will try to enhance the capability of our IDS by making it more robust to detect the intrusions of all the types and to overcome the damage caused to the system during the hacking or intruding phase. The IDS capability to withstand more dynamic threats is to be enhanced more in future and will propose a algorithm which can be enhanced more in terms of Quality of Service and minimizes the time delay and network routing load involved in computation and verification of security fields during route discovery process and performs better than the original AODV protocol in the presence of malicious nodes.

REFERENCES

[1]. A. Kush and S. Taneja, "A Survey of Routing Protocols in Mobile Adhoc Network", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp 279-285, August 2010.

[2]. C. E. Perkins, Adhoc Networking, Addison-Wesley, March 2005.

[3]. C. E. Perkins, E. B. Royer and S. Das, "Adhoc On-Demand Distance Vector (AODV) Routing", IETF Internet Draft, July 2003.

[4]. Ashwani Kush, "Security and Reputation Schemes in Ad-Hoc Networks Routing", International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp. 185-189, January June 2009.

[5]. A. Kush "Security Aspects in AD hoc Routing", Computer Society of India Communications, Vol. no 32 Issue 11, pp. 29-33, March 2009.

[6]. B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[7]. D. B. J., Yih-Chun Hu, Adrian Perrig, "Ariadne: A secure on-demand routing protocol for ad-hoc networks", Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.

[8]. L. Zhou and Z. J. Haas, "Securing ad hoc networks", IEEE Network Magazine, 13(6):24–30, November/ December 1999.

[9]. P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[10]. Wenjia Li, Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, http://www.cs.umbc.edu/~wenjia1/ 699_report.pdf, 2008

[11]. Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, Dec. 2001.

[12]. Y.-C. Hu, D.B. Johnson, A. Perrig, 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3–13, IEEE, Calicoon, NY, June 2002.

[13]. M.G.Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF Network Working Group, Internet Draft, 2005, http://tools.ietf.org/html/draft-guerrero-manet-saodv-04.

[14]. B.Dahill, B.N.Levine, E.Royer and C.Shields, "ARAN: A Secure Routing Protocol for Ad hoc Network", UMass Tech Report, pp. 02-32, 2002.

[15]. Seung Yi, Prasad Naldurg, Robin Kravets, "Security-Aware Ad-hoc routing for wireless networks", Technical Report No. UIUCDCS-R-2001-2241, August 2001 and In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing 2001, Long Beach, CA, USA, October 04 - 05, 2001.