Global Journal of Computer Science & Technology
Volume 11 Issue 6 Version 1.0 April 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Security Analysis of Routing Protocols

By J.Viji Gripsy , Dr. Anna Saro Vijendran

Abstract- : Mobile ad hoc networking (MANET) is gradually emerging to be very important in the growth of wireless technology. This is anticipated to offer a range of flexible services to mobile and nomadic users by means of integrated homogeneous architecture. The proper routing protocol is necessary for better communication in MANET. One of the existing reliable protocols is Ad Hoc On-Demand Vector Routing (AODV) protocol which is a reactive routing protocol for ad hoc and mobile networks that maintains routes only between nodes that wants to communicate. There are various security issues to be considered in this protocol. In order to provide security for AODV protocol, Secure Ad Hoc On-Demand Vector Routing (SAODV) can be used. SAODV is an extension of the AODV routing protocol that can be used to shield the route discovery process by providing security characteristics like integrity and authentication. For secure protocol, digital signature, hash chains, etc., can be used in routing. This paper surveys on various techniques available for securing the mobile ad hoc network.

Keywords: *Mobile Ad-hoc Network, Routing Protocols,AODV protocol, SA-AODV protocol*

Classification: *GJCST Classification: C.2.2*

Strictly as per the compliance and regulations of:

A Survey on Security Analysis of Routing Protocols

J.Viji Gripsy[α], Dr. Anna Saro Vijendran[Ω]

Abstract- Mobile ad hoc networking (MANET) is gradually emerging to be very important in the growth of wireless technology. This is anticipated to offer a range of flexible services to mobile and nomadic users by means of integrated homogeneous architecture. The proper routing protocol is necessary for better communication in MANET. One of the existing reliable protocols is Ad Hoc On-Demand Vector Routing (AODV) protocol which is a reactive routing protocol for ad hoc and mobile networks that maintains routes only between nodes that wants to communicate. There are various security issues to be considered in this protocol. In order to provide security for AODV protocol, Secure Ad Hoc On-Demand Vector Routing (SAODV) can be used. SAODV is an extension of the AODV routing protocol that can be used to shield the route discovery process by providing security characteristics like integrity and authentication. For secure protocol, digital signature, hash chains, etc., can be used in routing. This paper surveys on various techniques available for securing the mobile ad hoc network.

Keywords: Mobile Ad-hoc Network, Routing Protocols, AODV protocol, SA-AODV protocol

I. Introduction

An ad hoc network is usually defined as an infrastructureless network. This means that a network is lacking the standard routing infrastructure like fixed routers and routing backbones. Usually, the ad hoc nodes are mobile and the fundamental communication medium is wireless. Every ad hoc node possibly will be able to of act as a router. Such ad hoc networks may arise in personal area networking, meeting rooms and conferences, disaster relief and rescue operations, battlefield operations, etc.

By considering the special characteristics of MANET, designing a well-organized and dependable routing protocol strategy is a huge challenge. Currently, various ad hoc routing protocols have been proposed and developed by various researchers like DSDV, OLSR, TBRPF, AODV, DSR and ZRP. From all these, Ad-hoc On-demand Distance Vector (AODV) is recognized as one of the main IETF standards for MANET routing. On the other hand, AODV aims on improving routing performance, but provides only slight consideration to routing security, which indicates that it is susceptible to various attacks from malicious, compromised and selfish nodes.

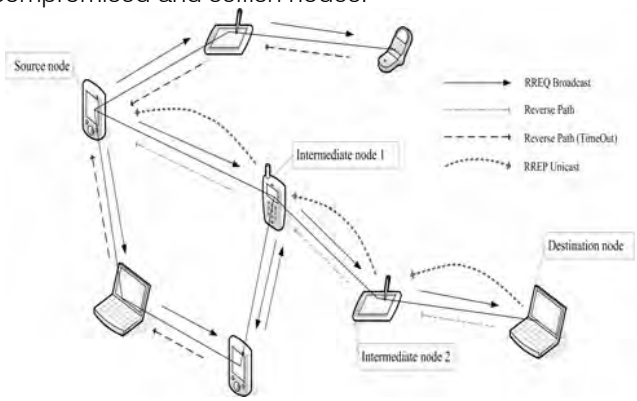

Figure 1: Route Discovery Procedure of AODV Protocol

AODV protocol is a reactive routing protocol for ad hoc and mobile networks. This represents that AODV will not perform any action until a node requires broadcasting a packet to a node for which it does not know a route. In addition, it only maintains routes among nodes that require communicating. Its routing messages do not enclose information about the entire route path, but simply regarding the source and the destination. Hence, routing messages have a constant size, independently of the number of hops of the route. It utilizes destination sequence numbers to indicate how fresh a route is that is used to grant loop freedom.

In AODV, a node performs route identification by flooding the network with a 'Route Request' message (RREQ). When it arrives a node that knows the requested route, it reply with a 'Route Reply' message (RREP) that goes back to the creator of the RREQ. Next, all the nodes of the identified path have routes to both ends of the path. Beside these routing messages, 'Route Error' messages (RERR) are utilized to alert the other nodes that several nodes are not any longer reachable because of link breakage. The route discovery procedure of AODV protocol is provided in figure 1.

But AODV lacks security features which lead to great vulnerability for attacking. To provide security for AODV, Secure Ad Hoc On-Demand Vector Routing (SAODV) s used which focuses on using various techniques like digital signature, hash chains, etc., This paper focuses on analyzing various security enabled protocols for providing better security for MANET.

About[α]- Assistant Professor, Ph.D Research Scholar , Department of Computer Science, PSGR Krishnammal College for Women,Pursuing my Phd in SNR SONS COLLEGE ,COIMBATORE,INDIA.
Email : gripsyjebs@gmail.com
About[Ω]- Director, Department of Computer Applications SNR SONS College, Coimbatore, India.

II. Literature Survey

As AODV lacks security mechanisms, malicious nodes can carry out several attacks just by not behaving based on the AODV rules. Therefore, to guarantee the entire security of the network, it is important to create security mechanisms that can withstand malicious attacks from insiders who have entire control of several nodes. For the purpose of protection against insider attacks, it is required to realize how an insider can attack a wireless ad-hoc network. Various attacks have been discussed in various literatures. According to the composition of operations for carrying out attack as mentioned in above article, misuses of AODV have been divided into two categories: atomic misuses and compound misuses. Intuitively, atomic misuses are carrying out by controlling a single routing message that cannot be any more separable. On the contrary, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol. Initially, it is required to determine a number of misuse goals that an inside attacker may require to achieve and are listed as follows.

Route Disruption (RD): Route Disruption is nothing but either breaking down an existing route or preventing a new route from being created.

Node Isolation (NI): Node isolation indicates the preventing of a provided node from communicating with any other node in the network. It varies from Route Disruption in that Route Disruption is targeting at a route with two provided endpoints, while node isolation is intended at every possible routes.

Route Invasion (RI): Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.

Resource Consumption (RC): Resource consumption is nothing but consuming the communication bandwidth in the network or storage space at every nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network. As an example, route disruption, route invasion and node isolation has been shown diagrammatically using figure 2, 3 and 4 respectively.

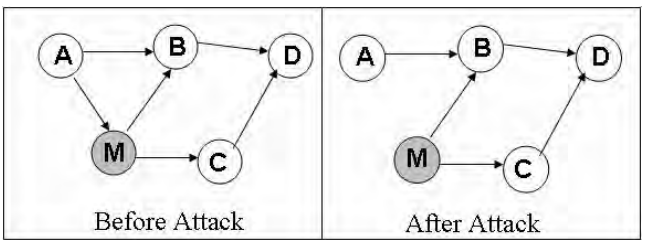

Figure 2: Node M performing Route Disruption for path A-C

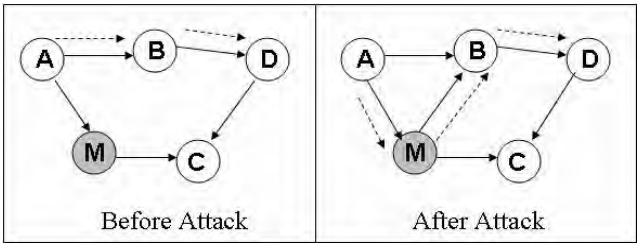

Figure 3: Route invasion

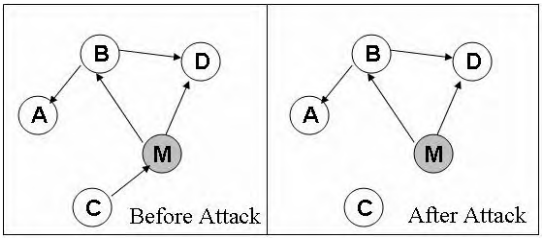

Figure 4: Node isolation

Investigation of atomic misuses can be carried out in an effective manner by means of understanding the causes of probable atomic misuse actions. All atomic misuse action is an inseparable manipulation of one routing message. In particular, the atomic misuse actions in AODV have been divided into the following four categories:

Drop (DR): Here, the attacker just drops the received routing message.

Modify and Forward (MF): Once the routing message is received, the attacker alters one or more fields in the message and then forwards the message to its neighbors through unicast or broadcast.

Forge Reply (FR): The attacker sends a faked message in reply to the received routing message. Forge Reply is generally related to the misuse of RREP messages that are in response of RREQ messages.

Active Forge (AF): The attacker sends a faked routing message without receiving any associated message.

The most interesting and complex one is that an attacker can merge several atomic misuses in a planned way and launch them.

Perlman [8] provides a link state routing protocol that attains Byzantine Robustness. Even though the protocol is greatly robust, it needs a very high overhead linked with public key encryption. Secure BGP [9] aims to protect the Border Gateway Protocol by using PKI (Public Key Infrastructure) and IPsec.

Zhou *et al.,* [10] primarily discuss key management for securing ad hoc networks. The author offers a section to secure routing, but basically conclude that nodes can shield routing data in the same manner they shield data traffic. They also examine that denial-of-service attacks against routing will be considered as damage and routed around.

Dahill *et al.,* [11] presented ARAN, a routing protocol for ad hoc networks that utilizes authentication

and needs the utilization of a trusted certificate server. In ARAN, each node that forwards a route discovery or a route reply message should also sign it. Additionally, it is implemented to reply attacks by means of error messages if not the nodes contain time synchronization.

Papadimitratos *et al.,* [12] put forth a protocol (SRP) that can be used to various available routing protocols particularly DSR and IERP. SRP needs that, for all the route discovery, source and destination should contain a security association among them. In addition, the author does not even refer to route error messages. Hence, they are not sheltered, and any attackable node can just create error messages by considering other nodes as source.

Hash chains are utilized in better manner for obtaining good authentication in various techniques that attempts to protect routing protocols. In [13], [14] and [15], hash chains are used for the purpose of providing delayed key disclosure. Whereas in [16], hash chains are utilized to generate single-time signatures that can be checked instantly.

In SEAD, hash chains are utilizes in grouping with DSDV-SQ [18] by Hu *et al.,* [17]. For each provided time all node contains its individual hash chain. The hash chain is separated into segments; elements in a segment are helpful in securing hop counts in a same manner as it is performed in SAODV. The size of the hash chain is identified when it is created. Following the usage of every elements of the hash chain a new one should be calculated. SEAD can be utilized with some appropriate authentication and key distribution techniques. However determining such a technique is not simple. Brijesh [19] discusses attacks against distance vector routing protocols and describes techniques to secure them using Message Authentication Codes.

Songbai *et al.,* [1] proposed a SAODV which is a MANET routing protocol that can withstand black hole attack. AODV is a broadly used network routing protocol for MANETs. The propose of AODV shows some concentration to security issues, therefore consequential in the defenselessness of such MANET to the black hole attack. Based on AODV, the author suggested and realizes AODV suffering black hole attack - BAODV (Bad Ad Hoc On-demand Distance Vector Routing suffering black hole attack) that can imitate black hole attack to MANET by one of nodes as a malicious one in network. BAODV can be considered as AODV that is utilized in MANET which suffers from black hole attack. According BAODV, author also presents a secure and effective MANET routing protocol, the SAODV protocol that focuses on dealing with the security flaws of the AODV protocol and is accomplished to overcome the black hole attack.

Papadimitratos *et al.,* [2] deal with the security issues of route discovery in mobile ad hoc networks, providing a lightweight, however robust, routing protocol, the distance-vector secure routing protocol (DV-SRP). DV-SRP identifies on-demand multiple routes that are utilized among the network, devoid of clearly offering network connectivity. DV-SRP merges the merits of the kind of route discovery initially provided by AODV with security and therefore flexible to opposition that interrupt route discovery.

Pirzada *et al.,* [3] proposed a secure routing with the AODV Protocol. Because of their enhanced nature, ad-hoc networks are often utilized in non-secure situation that formulates them vulnerable to attacks. These attacks are offered by chipping in the malicious nodes adjacent to various network services. Routing protocols that work as the necessary force in these networks are a general target of these nodes. AODV is the commonly utilized routing protocols that are presently experiencing extensive research and development. AODV is in accordance with the distance vector routing, excluding the updates are shared not based on a periodic origin but on an as per accordance with the needs. The control packets enclose a hop-count and sequence number field that finds the freshness of routing updates. Since these fields are changeable, it generates a possible weakness that is often exploited by malicious nodes to advertise good routes. Likewise, broadcasting of routing updates in clear text also reveals vital data about the network topology that is once more a possible security hazard. The author provides a novel and pragmatic technique for securing the ad-hoc on-demand distance vector routing protocol that guards against a number of attacks performed against mobile ad-hoc wireless networks.

Sanzgiri *et al.,* [4] proposed authenticated routing for ad hoc networks. Initially, only the issue of offering effective techniques for finding paths in very dynamic networks was considered, without considering security. Since security is not considered, there are a various treats that can be used to influence the routing in an ad hoc network. The author describes these threats in this paper, particularly explaining their effects on ad hoc on-demand distance vector and dynamic source routing. Authenticated Routing for Ad hoc Networks (ARAN) protocol is proposed in this approach which uses public-key cryptographic techniques to counter all the attacks. ARAN can provide secure routing in environments where nodes are authorized to participate but in situations where participants are not to be authorized, it does not respond. The simulation and experimentation of the proposed ARAN clearly shows that the performance of the proposed approach is very significant in finding secure routes within an ad hoc network.

Khan *et al.,* [5] provided a security Adaptive Protocol Suite: Ranked Neighbor Discovery (RND) and Security Adaptive AODV (SA-AODV). Due to the raise in popularity and demand of mobility and ad hoc networking, weakness of wireless networks is also becoming a crucial issue. This study focuses on the security aspects of wireless communication, and proposes a technique with an enhanced security features. The proposed RND and SA-AODV routing protocol provides best solution for the security problems the neighbor discovery and the routing protocol for transmission are also included in this proposed approach. Based on distance metrics, the neighbor discovery phase contains the determination of trusted neighbors, which leads to trust ranking. This routing protocol provides a security adapted route from the source to its destination based on the trusted neighbors, and the required security level. The key benefit of this proposed approach is that a route is obtained with a user-defined level of security for a specific application. Thus the tow routing protocols provides a total solution for a secured environment for wireless transmission with security features.

Gurrero Zapata *et al.,* [6] suggested Securing Adhoc Routing Protocols. The problem of integrating security methods into routing protocols for ad hoc networks is considered in this paper. Security solutions like IPSec are not appropriate. A security mechanism for AODV to protect its routing information is considered in this paper. The author also discusses about the application of the proposed approaches to other similar routing protocols. Moreover, how a key management method could be used in combination with the proposed solution is also discussed in this paper.

Davide *et al.,* [7] proposed a securing AODV: the A-SAODV secure routing prototype. Mobile ad hoc networks create new type of security issues, resulted by their characteristics of collaborative and open systems and by restricted accessibility of resources. In this paper, the author considers a Wi-Fi connectivity data link layer as a basis and deals with routing security. The author elaborates the implementation of the secure AODV protocol extension that includes tuning approach which is intended at enhancing its performance. The author provides an adaptive method that enhances SAODV behavior. In addition, the author examines the adaptive strategy and another method which delays the confirmation of digital signatures.

Table 1. Overview of Existing Techniques

Method	Overview
[1]	Withstand Black Hole attack.
[2]	More robust and efficient in eliminating disrupt route discovery.
[3]	Guards against a number of attacks performed against mobile ad-hoc wireless networks.
[4]	Uses public-key cryptographic techniques to counter all the attacks. Very significant in finding secure routes within an ad hoc network.
[5]	Based on distance metrics, the neighbor discovery phase contains the determination of trusted neighbors, which leads to trust ranking. Route is obtained with a user-defined level of security for a specific application.
[6]	Usage of Key Management.
[7]	Some enhancement is performed in SAODV to improve the performance
[11]	ARAN, a routing protocol for ad hoc networks that utilizes authentication and needs the utilization of a trusted certificate server.
[13], [14], [15]	Usage of Hack chains for security.
[19]	Message Authentication Codes used for Security.

The overview of existing secure routing protocol is provided in table 1. These available techniques will helps in understanding the actual problems existing in developing the secure protocol. By analyzing those existing protocols, some techniques like digital signature, hash chains, etc., can be used together to achieve better secure routing protocol.

III. Conclusion

Mobile Ad Hoc Network is a multi-hop wireless network of mobile nodes, structuring a temporary network with no help from several recognized infrastructure or centralized administration. Because of the lack of some committed routers, each node needs to donate towards the configuration and protection of the routing framework. As there are no centrally administered secure routers, attackers can attack the network with ease. To overcome this better routing protocol must be used. AODV is the widely used routing protocol for MANET. But this protocol fails to deliver security benefits. For providing security to MANET, SAODV is used as routing protocol for MANET. This involves the usage of digital signature, hash chains, etc., In this paper, a survey is performed on the existing routing protocols for MANET. Mainly their security support is analyzed which helps for developing better security enabled routing protocol.

References Références Referencias

1. Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, Vol. 2, Pp. 421-425, 2009.
2. Papadimitratos, P. and Haas, Z.J., "Secure On-Demand Distance Vector Routing in Ad Hoc Networks", IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, Pp. 168-171, 2005.
3. Pirzada, A.A. and McDonald, C., "Secure Routing with the AODV Protocol", Asia-Pacific Conference on Communications, Pp. 57-61, 2005.
4. Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M, "Authenticated Routing for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 3, Pp. 598-610, 2005.
5. Khan, R.H., Imtiaz-ud-Din, K.M., Faruq, A.A., Kamal, A.R.M. and Mottalib, A., "A Security Adaptive Protocol Suite: Ranked Neighbor Discovery (RND) and Security Adaptive AODV (SA-AODV)", International Conference on Electrical and Computer Engineering, Pp. 588-593, 2008.
6. Gurrero Zapata, M. and Asokan, N., "Securing Ad hoc Routing Protocols", Proceeding 1st ACM Workshop. Wireless Sec., Pp. 1-10, 2002.
7. Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communication Magazine, Pp. 120-125, 2008.
8. Perlman, R., "Fault-tolerant broadcast of routing information", In Computer Networks, Pp. 395–405, 1983.
9. Kent, S., Lynn, C., Mikkelson, J. and Seo, K., "Secure Border Gateway Protocol (S-BGP)", Real World Performance and Deployment Issues, 2000.
10. Zhou, L. and Haas, Z.J., "Securing Ad Hoc Networks", IEEE Network Magazine, Pp. 24–30, 1999.
11. Dahill, B., Levine, B.N., Royer, E. and Shields, C., "A Secure Routing Protocol for Ad Hoc Networks", Technical Report UM-CS-2001-037, University of Massachusetts, Departament of Computer Science, 2001.
12. Papadimitratos, P. and Haas, Z.J., "Secure Routing for Mobile Ad Hoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.
13. Hauser, R., Przygienda, A. and Tsudik, G., "Reducing the Cost of Security in Link State Routing", Symposium on Network and Distributed Systems Security, Pp. 93–99, 1997.
14. Cheung, S., "An Efficient Message Authentication Scheme for Link State Routing", 13th Annual Computer Security Applications Conference, Pp. 90–98, 1997.
15. Perrig, A., Szewczyk, R., Wen, V., Culler, D.E, and Tygar, J.D., "SPINS: Security Protocols for Sensor Networks", Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Pp. 189–199, 2001.
16. Zhang, K., "Efficient Protocols for Signing Routing Messages", Proceedings of the Symposium on Network and Distributed Systems Security, 2001.
17. Hu, Y.C., Johnson, D. and Perrig, A., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", 4th IEEE Workshop on Mobile Computing Systems and Applications, Pp. 3–13, 2002.
18. Broch, J., Maltz, D.A, Johnson, D.B., Hu, Y.C. and Jetcheva, J., "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Proceedings of the 4th Annual International Conference on Mobile Computing and Networking, Pp. 85–97, 1998.
19. Brijesh Kumar, "Integration of Security in Network Routing Protocols", SIGSAC Review, Pp. 18–25, 1993.

This page is intentionally left blank