Global Journal of Computer Science and Technology
Volume 11 Issue 16 Version 1.0 September 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Study on Enhancement of the Security of the Routing Protocols in Adhoc Networks

By C. Chandrasekar, Lt.Dr. S. Santhosh Baboo
Sree Narayana Guru College, Coimbatore , India

Abstract - An ad hoc wireless network is a set of wireless mobile nodes that self-configure to build a network without the requirement for any reputable infrastructure or backbone. Mobile nodes are utilized by the Ad hoc networks to facilitate effective communication beyond the wireless transmission range. As ad hoc networks do not impose any fixed infrastructure, it becomes very tough to handle network services with the available routing approaches, and this creates a number of problems in ensuring the security of the communication. Majority of the existing ad hoc protocols that deal with security issues depends on implicit trust relationships to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and nonrepudiation should not be compromised in any circumstances. Thus, security in ad hoc networks becomes an active area of research in the field of networking. There are various techniques available in the literature for providing security to the ad hoc networks. This paper focuses on analyzing the various routing protocols available in the literature for ad hoc network environment and its applications in security mechanisms.

GJCST Classification : H.2.8, D.2.9

Strictly as per the compliance and regulations of:

A Study on Enhancement of the Security of the Routing Protocols in Adhoc Networks

C. Chandrasekar[α], Lt.Dr. S.Santhosh Baboo[Ω]

Abstract - An ad hoc wireless network is a set of wireless mobile nodes that self-configure to build a network without the requirement for any reputable infrastructure or backbone. Mobile nodes are utilized by the Ad hoc networks to facilitate effective communication beyond the wireless transmission range. As ad hoc networks do not impose any fixed infrastructure, it becomes very tough to handle network services with the available routing approaches, and this creates a number of problems in ensuring the security of the communication. Majority of the existing ad hoc protocols that deal with security issues depends on implicit trust relationships to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and nonrepudiation should not be compromised in any circumstances. Thus, security in ad hoc networks becomes an active area of research in the field of networking. There are various techniques available in the literature for providing security to the ad hoc networks. This paper focuses on analyzing the various routing protocols available in the literature for ad hoc network environment and its applications in security mechanisms.

I. Introduction

An ad hoc network [1] is an infrastructureless network in which the nodes themselves are accountable for routing the packets. In the conventional Internet, routers within the central parts of the network are owned by a few well known operators and are therefore assumed to be somewhat trustworthy. This statement cannot hold good in an ad hoc network as all nodes coming into the network are expected to involve in routing. As the links in general are wireless, the security that was obtained because of the difficulty of tapping into a network is lost. Moreover, as the topology in such a network can be extremely dynamic, conventional routing protocols can no be effective.

The routing protocol [2, 3] provides an upper limit to security in any packet network. If routing can be misdirected, the whole network will be affected greatly. The issue is inflated by the fact that routing generally depends on the trustworthiness of all the nodes that are participating in the routing process. It is very tough to differentiate compromised nodes from nodes that are suffering from bad links.

Author α : M.C.A., M.Phil., Assistant Professor, Sree Narayana Guru College, Coimbatore - 641 105, India.
E-mail : Chandrasekar2000@gmail.com
Author Ω : Reader, D.G.Vaishnav College, Chennai - 600 106, India.

Because of self organize and rapidly deploy capability, ad hoc can be used in various applications like battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other applications. Though security [4] [5] has long been a vital and active area of research in wired networks, the unique features of Mobile Ad hoc Networks (MANETs) offer a new collection of nontrivial difficulties to security design. These difficulties comprise open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. It is very tough to maintain security of MANETs in group communication as of multiple senders and multiple receivers.

Previous security research [6] [7] in routing protocol mainly focuses on the use of encryption technology to implement message authentication. These routing protocols rely entirely on a central authority. Moreover, the performance of on demand routing protocols is very less which leads to various attacks. Thus, none of these existing protocols specifies any effective security measures which leads to malicious routing operations.

The main objective of this paper is to discuss ad hoc routing security with respect to the area of security. Various routing protocols available in the literature are analyzed to provide better security to the routing in ad hoc networks.

II. Literature Survey

There is no centralized administration or fixed network infrastructure for the ad hoc network and thus nodes execute routing discovery and routing maintenance in a self-organized way. But, this flexible network topology suffer from various security problems and the existing routing protocols such as AODV has no effective measures to avoid themselves from being attacked. There are various secure routing protocol techniques available in the literature to defend the ad hoc networks. However, majority of these secure routing protocols require certain centralized units or some trusted third parties to provide digital certificates or monitor network traffics, which demolish the self-organization nature of ad hoc networks. In this paper, Zhiyuan et al., [8] propose a secure routing protocol based on the trust mechanism. Each node in this ad hoc network has its views about some other node's

reliability, which are acquired by directly communicating with other nodes or by integrating other node's recommendations. Then the node will determine whether to exchange routing data with another node based on its view about that node's reliability.

The growth and development of tele-communication has increased the need for mobility, wireless or mobile networks and this has given more attention to the wired networks. The upcoming networks has entirely different infrastructure and has various protocols and devices. The main aim of this approach is to assess the two secure routing protocols Ariadne and SAODV in the performance characteristics rather than security features under random way point and Manhattan grid mobility models. Naeem et al., [9] used and implement the extension of AODV that is Secure Ad-hoc On-demand Distance Vector routing protocol (SAODV) and the extension of DSR that is Ariadne in the network simulator 2 (NS-2). In this paper, these protocols are compared with the quality of service parameters like delay, jitter, routing overhead, route acquisition time, throughput, hop count, packet delivery ratio using Manhattan grid and random waypoint mobility models. This paper mainly focuses on finding out the payload a node has to pay to assure the good quality of service.

Communications in MANETs are becoming more malicious in traffic analysis because of the broadcast nature of wireless transmissions. Even though, there are various secure routing protocols, traffic analysis attacks are still not well addressed with those existing techniques. Certainly, these protocols concentrate on security of route maintaining and protecting against modification of routing data, which cannot prevent traffic analysis attack. Anonymity is one of the most vital techniques to resistant against the malicious traffic analysis. In this paper, Sheklabadi et al., [10] described an anonymous version of ARAN, which is one of the significant secure routing protocols, to offer anonymity and maintain security of nodes in MANETs. The proposed protocol is based on the integration of the anonymous communication along with security specifications of ARAN. The main contribution of this protocol is combining several anonymous functionalities such as identity privacy, location privacy and route anonymity together with security features of ARAN

In order to secure the MANET in adversarial environments, it is necessary to possibly detect and defend possible attacks on routing protocols, especially internal attacks, such as a Byzantine attack. Ming Yu et al., [11] proposed a novel technique that identifies internal attacks by using both message and route redundancy during route discovery. The route-discovery messages are secured by pairwise secret keys between a source and destination and some intermediate nodes along a route established by using public key cryptographic mechanisms. An optimal routing technique is also proposed with routing metric integrating both requirements on a node's reliability and performance. A node constructs the reliability on its neighboring node's depending on its observations on the behaviors of the neighbor nodes. These two techniques can be combine into existing routing protocols like Ad hoc On-demand Distance vector routing (AODV) and Dynamic Source Routing (DSR). The author presented an integrated protocol called Secure Routing against Collusion (SRAC), in which a node makes a routing decision depending on its trust of its neighboring nodes and the performance provided by them. The simulation results have shown the advantages of the proposed attack detection and routing algorithm over the existing technique.

MANETs has several kinds of security issues, caused by their nature of collaborative and open systems and by limited availability of resources. In this paper, Cerri et al., [12] consider a Wi-Fi connectivity data link layer as a fundamental technique and concentrates on routing security. The author discusses the implementation of the secure AODV protocol extension, which comprises of alteration policies aimed at enhancing its performance. The author proposed an adaptive technique that adjusts SAODV behavior. Furthermore, the author examined the adaptive technique and another approach that delays the verification of digital signatures. This paper sums up the experimental results collected in the prototype design, implementation, and tuning.

MANETs are a set of wireless mobile devices with limited broadcast range and resources, and no fixed infrastructure. Communication is attained by communicating data along suitable routes that are vigorously identified and maintained through collaboration between the nodes. Determining such routes is a major job, both from efficiency and security points of view. Recently, a security model tailored to the particular needs of MANETs was introduced by Acs, Buttyan, and Vajda. The novel feature of this security system is that it assures security under concurrent executions. A novel route discovery technique called endairA was also proposed, along with a claimed security proof within the same system. In this paper, Burmester et al., [13] described that the security proof for the route discovery algorithm endairA is faulty, and moreover, this approach is susceptible to a hidden channel attack. The author also examined the security framework that was used for route discovery and argued that composability is a vital feature for ever-present applications. Ultimately, some of the major security challenges for route discovery in MANETs are discussed.

Decentralized node admission is a vital and fundamental security service in MANETs. It is required to steadily cope with dynamic membership and topology in addition to bootstrap other considerable security primitives (such as key management) and services (such as secure routing) without the help of any centralized trusted authority. A perfect admission approach should have least interaction among MANET nodes, as connectivity can be unstable. Moreover, as MANETs are frequently consists of weak or resource-limited devices, admission should be capable in terms of computation and communication. Majority of the existing admission protocols are prohibitively costly and need heavy interaction among MANET nodes. In this paper, Saxena et al., [14] concentrates on a general type of MANET that is formed on a temporary basis, and present a secure, efficient, and a fully noninteractive admission technique geared for this type of a network. This admission protocol depends on secret sharing techniques using bivariate polynomials. The author also presents a novel approach that facilitates any pair of MANET nodes to proficiently create an on-the-fly secure communication channel.

Routing in ad hoc networks is different from infrastructure-based wireless networks. In ad hoc networks each node acts as a router and is accountable for organizing topological data and ensuring correct route learning. In spite of various secure routing algorithms, security in ad hoc networks is still a controversial area. In this paper, Afzal et al., [15] first investigate the security issues and attacks in existing routing protocols and then the design and analysis of a new secure on-demand routing protocol, called RSRP is presented which appropriates the problems declared in the existing protocols. Furthermore, unlike Ariadne, RSRP uses a very proficient broadcast authentication technique which does not need any clock synchronization and assists instant authentication.

Routing in ad hoc network is one of the fundamental issues in networking. An opponent can easily hack the information in the network by attacking the routing protocol. There are several techniques available for the security enhancement of ad hoc network. In this paper, Imani et al., [16] argued about the defects in an ad hoc routing protocol that called Ariadne. This paper demonstrates that the security evidence for the route discovery technique Ariadne is defective, and furthermore, this algorithm is susceptible to certain attacks. In order to solve the limitations of this protocol, a novel proposed approach is presented in the route discovery algorithm. The proposed approach in this paper adds the capability of the malevolent node detections to this protocol.

Multipath routing diminishes the penalty of security attacks obtaining from collaborating malevolent nodes in MANET, by increasing the number of nodes that an opponent must negotiate in order to take control of the communication. In this paper, various attacks that cause multipath routing protocols more susceptible to attacks than it is expected, to collaborating malevolent nodes are recognized. Kotzanikolaou et al., [17] proposed a novel On-demand Multipath routing protocol called the Secure Multipath Routing protocol (SecMR) and the author examine its security properties. The SecMR protocol can be easily combined in an extensive variety of on-demand routing protocols, such as DSR and AODV.

Hu et al., [18] propose a more forceful protocol, which is more powerful in terms of security associations. In this approach, it is assumed that security associations are present between all pairs of nodes (through authentic public or Tesla [19] keys, or by shared secret keys). This facilitates both the sender and the receiver to validate all the nodes on the selected routing path.

Papadimitratos et al., [20] assumed that, for effective secure routing, it is enough, if effective security association is established between the sender and the receiver. It is demonstrated that the author's proposal avoids a wide range of attacks, but the proposed protocol is still susceptible to certain active attacks [21]. The author proposed a protocol (SRP) that can be effectively applied to a wide variety of existing routing protocols. This protocol focuses on the security association between source and destination nodes. Intermediate nodes need not require cryptographic validation of the control traffic. It adds an SRP header to the base routing protocol (DSR or AODV) request packet. SRP header has three vital fields namely QSEQ, QID and SRP MAC. QSEQ facilitates to avoid replay of old outdated requests. QID and random number help to prevent fabrication of requests, and SRP MAC guarantees reliability of the packets in communication. In SRP, for every route discovery, it is necessary that the source and destination must have a security association between them. Moreover, this approach does not focus on the route error messages. Hence, they are not protected, and any malevolent node can just counterfeit error messages with other nodes as source.

ARIADNE [22] is based on DSR [23] and TESLA (on which its authentication approach is based). ARIADNE prevents attackers/compromised nodes from troublemaking uncompromised routes that consist of benign nodes. It employs highly effective symmetric key cryptography technique. ARIADNE does not offer effective security against passive attackers eavesdropping on the network traffic. It does not provide security from an attacker from inserting data packets. It is susceptible to active-1-1 attacker that lies along the identified route, which does not forward packets and does not cause error if it meets a broken link. It also needs clock synchronization, which is regarded as an unrealistic necessity for ad hoc networks.

Perlman proposed a link state routing protocol [24] that attains Byzantine strength. Though, the protocol is extremely forceful, it needs a very high operating cost associated with public key encryption. Zhou and Haas [25] chiefly describe key management in their paper to provide security to ad hoc networks. The author devotes a part to secure routing, but in essence concludes that "nodes can defend routing data in the similar way they protect data traffic". They also examine that denial-of-service attacks against routing will be considered as damage and it is routed around. Certain research has been done to secure ad hoc networks by means of misbehavior detection approaches. This technique has two major problems: Initially, it is fairly likely that it will be not possible to discover various kinds of misbehaving; and secondly, it has no real means to assure the integrity and authentication of the routing messages.

Dahill *et al.* [26] proposed ARAN. Managed open environment is considered in this approach, where there is an opportunity for pre-deployment of infrastructure. It consists of two distinctive stages. The first stage is the certification and end-to-end authentication stage. Here the source obtains a certificate from the trusted certification server, and then by means of this certificate, signs the request packet. Each intermediate node consecutively signs the request with its certificate. The destination then validates each of the certificates, hence the source and the intermediate nodes gets authenticated. The destination node then sends the reply through the route reverse to the one in the request; reply signed with the help of the certificate of the destination. The second stage is a non-compulsory stage which is used to identify the shortest path to the destination, but this stage is very costly. It is susceptible to reply attacks using error messages but for the nodes have time synchronization.

III. Problems and Directions

The lack of infrastructure and organizational setting of mobile ad-hoc networks creates unique chances to attackers. MANETs are generally organized without a central control unit; the devices in a MANET depend on other units to route data to their destinations. Moreover, MANET nodes are frequently constrained in power and this makes MANETs susceptible to several malevolent attacks and usage of the routing approaches that work with wired networks is infeasible.

It is the fact that secure ad hoc routing can be achieved at the expense of messages, time and computation power, and that the overhead stems mainly from the computation complexity of the cryptographic techniques employed in frequently repeated routing procedures.

The major factors that should be considered in the establishment of sufficient routing protocols are multi hop, mobility, large network size combined with device heterogeneity, bandwidth and battery power. In order to solve the challenging problem of routing in ad hoc wireless networks, a novel technique is needed. The field of artificial intelligence can provide significant solution to the security problems in routing. Specifically, techniques from Swarm Intelligence (SI) and many Optimization techniques can be taken into account.

IV. Conclusion

To establish a secure MANET routing protocol with multiple metrics is a challenging task, particularly as the network topology and traffic are dynamic and changing all the time. This chapter focuses on the routing protocols in the ad hoc networks. In this paper, the routing algorithms that support communications in mobile ad hoc networks are discussed. The majority of the existing routing protocols suffer from various drawbacks and efficient security is not given to the MANET. This survey on the secure routing protocols is very much useful for the enhancement of the other routing protocol techniques. These routing protocols are the source for the development of new routing protocols with better security and performance.

References References Referencias

1. Ismail M., "Routing Protocols for Ad Hoc Wireless Networks", M. Sc. (ISS) project, Carleton University, Ontario, Canada, 2001.
2. M. Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," in Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002, pp. 1–10.
3. L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 78-93, 2009.
4. Keng Seng Ng and Seah W. K. G., "Routing security and data confidentiality for mobile ad hoc networks", The 57th IEEE Semiannual Vehicular Technology Conference, 2003.
5. K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in Proceedings of IEEE ICNP, 2002.
6. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, 2002, pp. 70 75.
7. L. Venkatraman and D.P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," J. Parallel Distrib. Comp., 2002.
8. Zhiyuan Liu; Shejie Lu; Jun Yan; "Secure Routing Protocol based Trust for Ad Hoc Networks", Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Vol. 1, Page(s): 279 – 283, 2007.

9. Naeem, M.; Ahmed, Z.; Mahmood, R.; Azad, M.A.; "QOS based performance evaluation of secure on-Demand routing protocols for MANET's", International Conference on Wireless Communication and Sensor Computing, 2010, pages 1-6, ICWCSC 2010.
10. Sheklabadi, E. Berenjkoub, M. "An anonymous secure routing protocol for mobile ad hoc networks", 2011 International Symposium on Computer Networks and Distributed Systems (CNDS), page(s): 142 – 147, 2011.
11. Ming Yu Mengchu Zhou Wei Su "A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 58, No. 1, pages 449 – 460, 2009.
12. Cerri, D. Ghioni, A. "Securing AODV: the A-SAODV secure routing prototype", IEEE Communications Magazine, Vol. 46, No. 2, page(s): 120 – 125, 2008.
13. Burmester, M.; de Medeiros, B.; "On the Security of Route Discovery in MANETs", IEEE Transactions on Mobile Computing, Vol. 8, No. 9, Page(s): 1180 – 1188, 2009.
14. Saxena, N.; Tsudik, G.; Jeong Hyun Yi; "Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs", IEEE Transactions on Parallel and Distributed Systems, Vol. 20, No. 2, Page(s): 158 – 170, 2009.
15. Afzal, S.R.; Biswas, S.; Jong-bin Koh; Raza, T.; Gunhee Lee; Dong-kyoo Kim; "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks", IEEE Wireless Communications and Networking Conference, page(s): 2313 – 2318, 2008. WCNC 2008.
16. Imani, M.; Taheri, M.; Rajabi, M.E.; Naderi, M.; "A secure method on a routing protocol for ad hoc networks", 2010 International Conference on Educational and Network Technology (ICENT), page(s): 482 – 486, 2010.
17. Kotzanikolaou, P.; Mavropodi, R.; Douligeris, C.; "Secure Multipath Routing for Mobile Ad Hoc Networks", WONS 2005. Second Annual Conference on Wireless On-demand Network Systems and Services, Page(s): 89 – 96, 2005.
18. Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of MobiCom, September 2002.
19. A. Perrig, R. Canetti, J.D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. RSA CryptoBytes, 5(Summer), 2002.
20. P. Papadimitratos and Z.J. Haas. Secure Routing for Mobile Ad Hoc Networks. In Proceedings of CNDS, January 2002.
21. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of IEEE Infocom, April 2003.
22. 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 (2001).
23. D. B. Johnson et al., "The dynamic source routing protocol for mobile ad-hoc networks (DSR)", Internet draft, MANET Working Group (2002).
24. R. Perlman, Fault-tolerant broadcast of routing information, Computer Networks, 7, 395–405 (1983).
25. L. Zhou, and Z. J. Haas, Securing ad-hoc networks, IEEE Network Mag., 13, 24–30 (1999).
26. B. Dahill, B. N. Levine, E. Royer, and C. Shields, A secure routing protocol for ad-hoc networks, Technical Report UM-CS-2001-037, Department of Computer Science, University of Massachusetts (2001).

This page is intentionally left blank