International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Security Challenges & Routing Protocols in Manets

Sheikh Abdul Wajid*[1], Farah Fayaz Quraishi[2], Pummy Dhiman[3]
*[1]Lecturer , PG Department of Computer Sciences, University of Kashmir, Srinagar, India
[2]Research Scholar, PG Department of Computer Sciences, University of Kashmir, Srinagar, India
[3]Assistant professor, Department of Computer Sciences, Vidya Jyoti Eduversity, Derabassi Punjab, India

ABSTRACT

MANETs are group of mobile nodes that communicate in wireless medium using various underlying protocols. The communications are either single hop or multi hop. Due to various inherent characteristics of MANETs these are much more vulnerable to various types of attacks. Since the increased use of these types of networks mandates to have secure transmission of information between nodes so various secure routing protocols were proposed. This paper presents outline of various secured routing protocols in MANETs.

Keywords: RSA, SHARP, AODV, MANETs

I. INTRODUCTION

MANETs incorporates group of nodes which are self-organizing, mobile and infrastructure less in nature. The nodes are connected to form a network without any membership function that is any node can come and go in a network on the fly. The nodes communicate wirelessly without having any pre existing network. The nodes communicate either in single hop modes in which nodes communicate directly or in multi hop fashion in which intermediate nodes act as rely nodes from source to destination. Mobile adhoc networks are characterized by various features as having wireless nature of medium, changing topology and insure data transmission. Since the nodes in adhoc network are resource limited and are constrained by both computation power and energy which causes inconsistency in the links between the nodes. This in turn leads to the topology change in the network.

In the recent times there has been increased use of mobile adhoc networks, but due to insecure nature of communication there is a challenge to route secure data in this type of network. Since the increasing use of MANETs in sharing sensitive information has made it necessary to have securing routing protocols which will guarantee to share sensitive data in mobile adhoc networks. All the standard routing protocols have no built in security capability. The standard routing protocols can be enhanced to incorporate security function in them. The standard routing protocols can be classified as either proactive, reactive or hybrid routing protocols. The proactive routing protocols maintain dedicated communication channels between nodes.

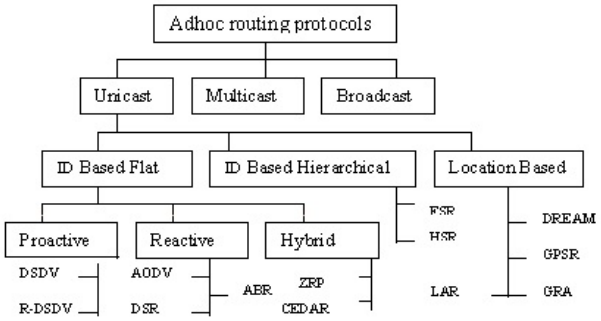

Figure 1. Classification of routing protocols in MANETs.

The reactive routing protocols built the communication channel on the fly as and when the communication between nodes is needed.

The hybrid routing protocols are best suited for massive networks by taking into account the radio transmission range of individual nodes.

The MANET protocols can also be categorized as unicast (data send between node to node), multicast (date send from node to a group of nodes) broadcast (data send to all nodes).

CLASSIFICATION OF ATTACKS ON MANETs

The MANETs are prone to security threats due to its characteristics as:

- Wireless transmission medium
- Lack of security mechanism in routing protocols
- Dynamic topology
- Lack of membership function

As the optimum security features are not provided by standard routing protocols, so manets are much more vulnerable to number of attacks either from external or internal entity. Also, since the increased use of MANETs for sharing the information there emerges much need to have some secure authenticated routing protocols. With the introduction of internet of things and the characteristics of MANETs like self configurable, robust than cellular networks, rapid deployable & less time consuming there has been increased use of adhoc networks that rely on infrastructure less type of network. Various types of routing protocols have been proposed which provide resistance against various types of attacks. In MANETs the attacks can broadly classified as:

External attacks: these attacks are carried out by the nodes outside the network, these nodes are not members of the network but they penetrate into the network in order to carry out the attack.

Internal Attack: these attacks are carried out by the nodes within the network. These nodes are compromised and are having malicious behaviour.

Passive Attack: In passive attacks continuous information is being collected without affecting the operation of the protocol. The valuable information is being filtered without altering the data packets to gather the required information. This type of attack is much difficult to identify as they don't disrupt the communication pattern. The passive attacks may either as traffic analysis or eavesdropping.

Active Attacks

Active attacks are carried by actively interacting with the victim. The attacker may alters the information contained in data packets, drop the packets from source to destination, sleep deprivation of notes, routing false packets to cause congestion in network or unavailability of network channels. These attacks are very dangerous.

SECURITY ISSUES IN MANET

The main issues for providing security in MANET are briefly discussed below.

- Identification issue: nodes accessing common link can participate in setting ad hoc network infrastructure. But secure communication is based on secure paths between nodes.
- Authentication issue: Nodes must be able to verify identity of other nodes before having established secure communication link.
- Transmission issue: The credentials should not be compromised at the recipient node.
- Privacy Issue: identification issue simultaneously leads to privacy issue for MANET. A compromised node leads to privacy threat to a particular node.

Therefore, due to the issues discussed above, it is essential to provide security architecture to secure ad hoc networking. In the literature, there are many works that address the security issues in MANETs.

II. LITERATURE REVIEW

The rapid increase in the demand of MANETs has necessitated the need for secure routing protocols, such that various types of attacks are averted. Panagiotis Papadimitratos, Zygmunt J. Haas proposes secure link state routing protocol based on secure proactive topology discovery. This protocol is robust against Dos attacks and byzantine adversaries[1]. Yih-Chun Hu ,David B. Johnson , Adrian Perrig proposed secure efficient ad hoc distance vector routing protocol based on DSDV. It uses hash function to provide guard against DOS. Destination sequence numbers provide reply attack protection[2]. Manel Guerrero Zapata proposes SAODV an enhancement of AODV has security features of integrity and authentication[3]. Abdalla Mahmoud Ahmed Sameh Sherif El- Kassas proposes ARAN an on demand secure routing protocol based on digital certificates. It provides authentication, integrity and non-repudiation[4]. John Marshall et al. [6] proposed protocol using SRP algorithm for ANET routing. Oscar F. Gonzalez et al. [7] proposed mechanism that identifies malfunction and denial of services by nodes. Stephan Eichler et al. [8] proposed secure routing protocol for vehicular MANETs based on underlying AODV. M. Rajesh Babu et al. [9] have proposed an energy efficient secure authenticated routing protocol (EESARP). Steffen Reidt et al. [10]

have introduced a trust metric in the cluster head selection process to securely determine constituting nodes in a distributed Trust Authority (TA) for MANETs. Muhammad Nawaz Khan et al. [11] have proposed distributed-ID, a smart agent in each mobile node analyzes the routing packets. Lu Jin et al. [12] introduced the secure the delivery of routing packets and the strategy to determine the most secure routes. Panagiotis Papadimitratos et al. [13] have proposed the securing the delivery of routing packets and the strategy of determine the most secure routes. Shivasharanappa Allur et al. [14] have proposed a cross-layer design to achieve an unswerving data transmission in ADHOC networks. Venkat Balakrishnan et al. [15] introduced Trust Enhanced security Architecture for MANET (TEAM), in which a trust model is overlaid on the following security models key management mechanism, secure routing protocol, and cooperation model. [5] have addressed anonymity and trust issues for a wireless network containing selfish and malicious nodes.

Remya S & Lakshmi K S [16] proposed anonymous routing protocol for MANETs. This paper proposes Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. SHARP is cluster or group based anonymous routing protocol. S. Kalai Selvil, V. Ganeshkumar [17] proposed energy efficient routing protocol To provide high anonymity protection at a low cost, the authors have proposed Energy-aware Anonymous Routing protocol (EARP). EARP dynamically partitions the network area into zones and randomly chooses nodes in zones as intermediate Relay Nodes (RN), which form a non-predictable anonymous route. EARP offers anonymity protection to sources, destinations, and routes. S. Imran, R. V. Karthick, P. Visu [23] This paper has studied and discussed about the various existing protocols and how efficient they are in the attacking environment. In this paper the authors have proposed a new concept by combining two proposed protocols based on geographical location based: ALERT which is based mainly on node-to-node hop encryption and bursty traffic. And Greedy Perimeter Stateless Routing (GPSR), a new geographical location based protocol for wireless networks that uses the router's position and a packet's destination to make forwarding of packets. Rangara, R.R., Jaipuria, R.S., Yenugwar, G.N., Jawandhiya, P.M[22] proposes a scheme that employs multiple routing protocols. As different routing protocols are prone to different types of attacks, the idea proposed is to switch the routing protocol upon a particular type of attack detected on the network. The solution detects three types of attacks: black hole, routing table overflow and sleep deprivation torture attack. Seys, S., Preneel, B [24] proposes ARM, an anonymous routing scheme that is based on a trapdoor generated using one-time pseudonyms. Pseudonyms can be generated using counters or synchronized clocks. Li, X., Li, H., Ma, J., Zhang [25] also proposes an efficient anonymous routing protocol called EARP. The protocol is based on onion routing where every roué request and reply message is encrypted with a trust key. A Hello message is sent back to the source during discovery to confirm the node a trusted node to ancestor. Hong, J.K.A.X [27] proposes ANODR[28] was the first anonymous routing protocol proposed for MANET. It is assumed that source and destination shares a secret key. During route discovery, the source generates a trapdoor identifier by encrypting a message "you are destination" with the the shared key. Raj, P.N., Swadas, P.B [23] proposes a scheme called DPRAODV to detect black hole attack based on the sequence number of RREP packets. If the sequence number is higher than a threshold, the node is marked as blacklisted. In this case, an ALARM message is generated to notify other nodes. Buttya, A.G.L., Vajda, I.N [26] proposes endairA[29] is an inspiration of Ariadne protocol. N. W. Lo, M. C. Chiang, C. Y. Hsu [18] proposes Hash-based Anonymous Secure Routing protocol (HASR) for MANETS, whose design is based on collision-resistant one-way hash function and pseudo-name generation/exchange mechanism. Since no key cryptography or cryptographic onion mechanism is used in our protocol, HASR spends far more less computation time and network bandwidth during routing operations in comparison with existing solutions. M. Khatkar, N. Phogat, B. Kumar [19] proposes Alarm protocol is Anonymous Location-Aided Routing in MANET. It is based upon proactive and link-state routing. It constructs a secure MANET map using Nodes' current Location using LAM. Location information has available through GPS receivers. A. Vijayan, C. Yamini [20] proposes anonymous routing protocol with RSA encryption technique, so that we use AODV routing protocol for the on-demand application. The private key generation is the major security traits with encryption. Our proposed protocol ART will detect and provide protection from attackers. K. V. Arya, R. Saxena [21]

proposes anonymous routing protocol known as S-ALERT. In order to provide anonymity without compromising the security, we have extended Anonymous Location Based Efficient Routing Protocol (ALERT) to make it secure. The secure version is named as Secure Anonymous Location Based Efficient Routing protocol (S-ALERT). S-ALERT uses Suspect Detection algorithm to choose the nodes in a route which provide unperceivable route.

Most of routing protocols proposed can't provide all the anonymity together. Most of them are location based. They are using geographical routing protocols (Example – Greedy Perimeter Stateless Routing Protocol) as underline protocol. ALARM, ZAP, SDDR, ALERT are some of the existing anonymous routing protocols. Greedy Perimeter Stateless Routing (GPSR) is a simplified variant of the GFG protocol. ALARM cannot provide the location of sender and receiver, SDDR lacks the route privacy, and ZAP concentrates only on destination privacy.

III. SCOPE FOR FUTURE ENHANCEMENT

Secure routing protocols may be developed in near future which will mainly focus to enhance security and quality of service of the protocols. Achieving these two parameters might be challenging at times as incorporating security adds routing overhead to the protocol which might degrade its routing efficiency. So, there needs to have optimum trade off for protocols between these two parameters. The routing overhead due to encryption algorithm should not imply negative impact on its performance. One such protocol discussed above is SHARP[16] which achieves security by transmitting RSA encrypted data between clusters thus achieving inter cluster security. However, if the node within the cluster is compromised it can not be detected. So there can be addition of a security layer for intra cluster data transmission. The active or passive attacks can also be detected by having acknowledgment to the sender node.

IV. CONCLUSION

This paper presents an overview of various types of attacks in MANETs and the key challenges in mobile adhoc networks. The protocols proposed to address the security concerns were analysed in detail. The secure protocols are mainly based on either proactive or reactive routing protocols. The security features added to the protocols were analysed to provide optimum security at limited resource usage. One such protocol was proposed for enhancement as enhanced secured hierarchical routing protocol in MANETs which is based on underlying AODV protocol.

V. REFERENCES

[1]. Panagiotis Papadimitratos, Zygmunt J. Haas " Secure Link State Routing for Mobile Ad Hoc Networks", Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on 27-31 Jan. 2003 Page(s):379 - 383,ISBN: 0-7695-1873-3

[2]. Yih-Chun Hu ,David B. Johnson , Adrian Perrig "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", 1570-8705/$ 2003 Published by Elsevier B.V. doi:10.1016/S1570- 8705(03)00019-2

[3]. Manel Guerrero Zapata:"Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" INTERNET-DRAFT draft-guerrero-manetsaodv-06.txt. September 2006.

[4]. Abdalla Mahmoud Ahmed Sameh Sherif El-Kassas, " Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed- ARAN)" 0-7803-9466-6/05/$20.00 ©2005 IEEE

[5]. R. Kalpana et al., Mobile Anonymous Trust Based Routing Using Ant Colony Optimization, IEEE Asia-Pacific Services Computing Conference (APSCC), 2010.

[6]. Marshall, j et al., Identifying flaws in the secure routing protocol. IEEE Conference on Performance, Computing, and Communications, 2003.

[7]. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad- Hoc Networks, Springer-Verlag Berlin Heidelberg 2007.

[8]. Eichler, S. et al., Secure Routing in a Vehicular Ad Hoc Network. IEEE Vehicular Technology Conference, Sep. 2004.

[9]. M. Rajesh Babu et al., An Energy Efficient Secure Authenticated Routing Protocol for Mobile Ad hoc Networks. International Journal of Reviews in Computing, Vol. 7, Sep. 2011.

[10]. Steffen Reidt et al., Efficient, Reliable and Secure Distributed Protocols for MANETs. 2nd

International Conference on Mobile Technology, Applications and Systems, Nov. 2005.

[11]. Muhammad Nawaz Khan et al., Intrusion Detection System for Ad hoc Mobile Networks. Int. Conf. on Information Technology: Research and Education, Jun.2005.

[12]. Lu Jin et al., Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad Hoc Network. Wireless Telecommunications Symposium, Apr. 2006.

[13]. Panagiotis Papadimitratos et al., How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET, IEEE-CS Broad Nets, San Jose, CA, USA, Oct. 2006

[14]. Shivasharanappa Allur et al., Efficient SNR/RP Attentive Routing Algorithm: Cross-Layer Design for Ad hoc Networks, IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), Oct.2006.

[15]. Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucs, TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks, IEEE International Conference on Networks, Nov. 2007, pp. 182-187.

[16]. Remya S, Lakshmi K S "SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs" , International Conference on Computer Communication and Informatics, 2015. IEEE.

[17]. S. Imran, R. V. Karthick, P. Visu, "DD-SARP: Dynamic data secure Anonymous Routing Protocol for MANETs in attacking environments" , International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015. IEEE

[18]. N. W. Lo, M. C. Chiang, C. Y. Hsu, "Hash-Based Anonymous Secure Routing Protocol in Mobile Ad Hoc Networks" , 10th Asia Joint Conference on Information Security (AsiaJCIS), 2015. IEEE.

[19]. M. Khatkar, N. Phogat, B. Kumar, "Reliable data transmission in Anonymous Location Aided Routing in MANET by preventing replay attack" , 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 IEEE.

[20]. A. Vijayan, C. Yamini, "Anonymous routing technique in MANETs for secure transmission: ART" , International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014. IEEE.

[21]. K. V. Arya, R. Saxena, "S-ALERT: Secure anonymous location-based efficient routing protocol" , 9th International Conference on Industrial and Information Systems (ICIIS), 2014. IEEE.

[22]. Rangara, R.R., Jaipuria, R.S., Yenugwar, G.N., Jawandhiya, P.M.: Intelligent Secure Routing Model For MANET. In: 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT (2010)

[23]. Raj, P.N., Swadas, P.B.: DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. IJCSI International Journal of Computer Science Issues 2 (2009)

[24]. Seys, S., Preneel, B.: ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks. International Journal of Wireless and Mobile Computing (2009)

[25]. Li, X., Li, H., Ma, J., Zhang, W.: An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks. In: Fifth International Conference on Information Assurance and Security (2009)

[26]. Buttya, A.G.L., Vajda, I.N.: Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing 5(11) (2006)

[27]. Hong, J.K.A.X.: ANODR: Anonymous On Demand Routing with Untraceable routes for Mobile Ad-hoc Networks. In: 4th ACM International Symposium on Mobile Ad hoc Networking and Computing, MOBIHOC 2003 (2003)

[28]. Sanzgiri, K. Dahill, B. Levine, B.N. Shields and C. Belding-Royer. A secure routing protocol for ad hoc networks. (ARAN) Network Protocols, 2002. Proceedings. 10th IEEE International Conference on ICNP'02

[29]. Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. International Conference on Mobile Computing and Networking. Proceedings of the 10th annual international conference on Mobile computing and networking.