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

Survey on Secure Routing Protocols for MANETs

Shwetha T R[1], Arun Biradar[2]

[1, 2]Computer Science and Engineering Department, VTU Belgaum, EWIT, Bangalore, India

Abstract: ***Mobile Ad hoc Networks (MANETS) are transient networks of mobile nodes, connected through wireless links, without any fixed infrastructure or central management. Due to the self-configuring nature of these networks, the topology is highly dynamic. This makes the Ad Hoc Routing Protocols in MANETS highly vulnerable to serious security issues. In this paper, we survey the common security threats and attacks and summarize the solutions suggested in the survey to mitigate these security vulnerabilities.***

Keyword: Ad-hoc network, MANET, Security attacks, Routing, Network Security Solutions

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a impermanent Network without the assistance of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-configuring and self-organizing multi hop wireless networks. Each node in mobile ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its communication range only. Nodes communicating usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not inside the transmission range of the source node, the source node takes help of the intermediate nodes in order to communicate with the destination node by relaying the messages hop by hop.

Mobile wireless networks are generally open to various attacks, such as information and physical security attacks than fixed wired networks. Securing wireless ad hoc networks is particularly more difficult for many of the reasons such as: vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology and etc. The wireless channel is accessible to both legitimate network users and malicious attackers. The abstract of centralized management makes the classical security solutions reliable on certification authorities and on-line servers not applicable. A malicious attacker can rapidly become a router and break network operations by deliberately not following the protocol specifications.

The nodes are free to move in any direction and organize themselves arbitrarily. They can join or leave the network at any time. Due to the frequently change in the network topology there is a significant change in the status of trust among different nodes which adds the complexity to routing among the various mobile nodes. The self-organization of nodes in ad hoc networks may tend to deny providing services for the advantage of other nodes in order to keep their own resources acquaint new security that are not addressed in the infrastructure-based networks.

2. Related Work

2.1 Security attacks

The security attacks in mobile ad hoc network fall into two categories: passive attacks and active attacks. In passive attack, malicious node does not affect the normal operation of data so it is very difficult to detect. It includes traffic analysis, monitoring and eavesdropping. Encryption algorithms are used to prevent passive attack s. In active attack, malicious node disrupts the normal functioning of system by performing either external or internal attacks. The threats for MANET's are classified as follows:

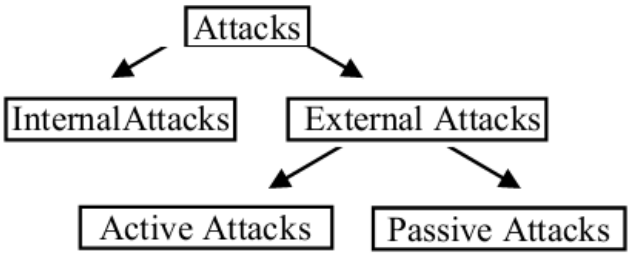

Figure 1: Attacks Classification

An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET. Examples include (Tomar et al., 2010; Goyal et al., 2010; Garg & Mahapatra, 2009; Wang, Hu & Zhi, 2008):

- Modification attacks
- Impersonation attacks
- Fabrication attacks
- Wormhole attacks
- Selfish behavior.

a) Modification Attacks: A modification attack is typically launched by a malicious node with the deliberate intention of redirecting routing packets, by for example modifying the hop count value of a routing packet to a smaller value. By decreasing the hop count value a malicious node can attract more network communication

b) Impersonation/Spoofing Attacks: In this type of attack (also known as spoofing) a malicious node uses for example the IP or ad-dress of another node in outgoing routing packets. As a result, the malicious node can receive packets

meant for the other node or even completely isolate it from the network.

c) Fabrication: The main purpose of fabrication attacks is to drain off limited resources in other MANET nodes, such as battery power and network connectivity by, for example, flooding a specific node with unnecessary routing messages. A malicious node can for example send out false route error messages. This kind of attack is more prominent in reactive routing protocols where path maintenance is used to recover broken links.

d) Wormhole Attacks: A wormhole (Hu et al., 2002c; Liu et al. 2007; Sanzgiri et al., 2002) is a particularly severe attack on MANET routing. A malicious node captures packets from one location in a network and tunnels them to another malicious node, located several hops away, which forwards the packets to its neighboring nodes. This creates the illusion that two endpoints of a Wormhole tunnel are neighbors even though they are located far away from each other in reality. A strategic placement of a wormhole causes most of the network traffic to pass through the malicious nodes which have formed the wormhole. Once the wormhole link has been successfully established, further attacks can be launched by the malicious nodes such as selective packet drop to disrupt communication or data sniffing to capture confidential information

e) Selfish Behaviour: This refers to a node which does not cooperate in any routing. It may for example, be that it wishes to save energy and so switches to a "sleep mode" whenever it is not taking part in any network communication. While such an attack may not be launched with explicitly bad intentions, it can lead to serious disruptions in network communications such as high route discovery delays and dropped data packets. If the selfish node also happens to be the only communication link between two MANET endpoints, communications between these endpoints will become unavailable.

2.2 Secure Routing Protocols for MANETs

Most routing protocols have been designed without taking security into account. It has been assumed that all nodes in a MANET are trusted. However, this is not the case in a large scale and dynamic MANET and if the routing protocol is unprotected, the whole MANET can be liable to several different types of security attacks. Much research has been done in the area of routing security in MANETs and several surveys on this research have been published (Abusalah, Khokhar & Guizani, 2008; Wang, Hu & Zhi, 2008; Djenouri & Badache, 2010; Singh, 2011). Due to the dominant status of reactive routing protocols for MANETs, most security research has tended to give attention to these protocols.

3. Cryptography based Secure Routing

In this subsection the cryptography-based secure routing protocols are presented.

a) Securing QoS Route Discovery (SQoS Route Discovery)

SQoS Route Discovery (Hu & Johnson, 2004) is a cryptographically protected version of QoS Route Discovery. SQoS Route Discovery relies entirely on symmetric cryptography.

Ariadne: Ariadne (Hu et al., 2002a) is a secure reactive (on-demand) routing protocol based on DSR that provides authentication of routing messages. Authentication can be performed by using shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. Ariadne is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol (Perrig et al., 2005) which is broadcast authentication procedure requiring relaxed time synchronization. It consists of two steps:

1. Authentication of routing messages
2. Verification that there is no node missing in the routing message headers

In step 1, if shared secrets are used, a node sending a routing request message indicates a message authentication code (MAC) which is computed with a shared secret key over a time stamp (or other unique data). The receiver of the message can then authenticate the message by using its own shared secret key.

In step 2, per-hop hashing is used to verify that no hop was omitted. Authentication of routing messages is not enough since an attacker could still remove a node from the list of intermediate nodes in a routing message. Ariadne though uses a one-way hash function to prevent this.

Ariadne provides good defense against modification, fabrication, and spoofing due to its message authentication and routing message header verification features. Ariadne can also provide protection from HM wormhole attacks, when used together with the TESLA Instant Key disclosure (TIK) protocol for precise time synchronization between neighbouring nodes, and PM wormhole attacks if the wormhole nodes do not have valid shared secrets.

c) Security Aware Ad hoc Routing (SAR)

The SAR protocol (Yi et al., 2001) incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the correct key can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have been travelled through nodes having the same trust level as the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route.

SAR has been presented as an extension to AODV but it can also be extended to any existing routing protocol. Due to strong cryptographic protection of routing messages, attacks such as modification, impersonation, and fabrication are effectively eliminated. A major problem with SAR, however, is that it involves significant encryption overhead since each intermediate node has to perform both encryption and decryption operations.

d) Authenticated Routing for Ad hoc Networks (ARAN)

The purpose of the ARAN protocol (Sanzgiri et al., 2002) is to detect and protect against malicious actions by third parties and peers. It provides authentication, message integrity, and non-repudiation. ARAN can be used in two different security stages: a simple mode which is mandatory and an optional stage which provides stronger security but also more overhead and is not suitable on mobile devices with very low processing or battery capacity. ARAN uses crypto-graphic certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbours. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own. Due to strong authentication, message integrity, and non-repudiation ARAN provides effective protection from modification, impersonation, and fabrication attacks. However, due to heavy asymmetric cryptographic operations and large routing packets, ARAN has a high computational cost for route discovery. ARAN is also vulnerable against selfish nodes that e.g. drop routing packets. In particular, if the selfish node is an authenticated node, then ARAN is unable to detect this type of attack.

e) Secure Efficient Ad hoc Networks (SEAD)

SEAD (Hu et al., 2002b) is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update message is verified by a receiving node. Looping is removed by using a sequence number and authentication of the source of routing update message. Authentication of the source can be done for example by providing a shared secret key between each pair of nodes in the MANET which is then used for MAC calculations between the nodes for the authentication of a routing update message. SEAD provides strong protection against attackers trying to create incorrect routing state in other nodes by for example modifying the sequence number in the routing packet. However, SEAD does not protect against an attacker tampering the next hop or the destination field of a routing update packet.

f) Secure Link State Routing Protocol (SLSP)

The main functionality of SLSP (Papadimitratos &Haas, 2003) is to secure the discovery and the distribution of link state information by using asymmetric keys. SLSP consists of three major steps: public key distribution, neighbour discovery, and link state updates. Public keys are distributed between a node and all its neighbours. A central server for key distribution is thus not needed. Periodic hello messages, used in neighbour discovery, are signed using the private key of the sender. Signed link state update messages are identified by the IP address of the initiating node and include a sequence number. A node receiving a link update messages verifies the attached signature using the public key it received earlier during the public key distribution phase. The hop count field in the update message is protected by using a one-way hash chain.

4. Conclusion

Routing security in infrastructure-less and self-configuring mobile networks, such as MANETs, has been highlighted as one of the most challenging security issues in current and future ubiquitous networks. Since there are a number of potential MANET security threats and many possible network environments (small, scalable, fixed, dynamic, homogeneous, heterogeneous, etc.) it is difficult to design a secure routing protocol providing protection from all types of attacks while at the same time being suitable for all types of MANET scenarios. A comparison of established secure routing protocols based on the classification is the main contribution in this paper. Further research needs to be undertaken both in in order to provide protection from all possible MANET routing attacks and for formulating recommendations on the selection of a secure routing protocol for a specific MANET, since no sing le currently proposed routing protocol provides protection against all forms of routing attacks in MANETs.

5. Acknowledgment

We express our heartfelt sincere gratitude to HOD of Computer Science and Engineering, East West Institute of Technology for his valuable suggestions and support. Special thanks to coordinator and guide for their valuable support and guidance.

References

[1] Abusalah, L., Khokhar, A., & Guizani, M. (2008). A Survey of Secure Mobile Ad Hoc Routing Protocols. IEEE Communications Surveys & Tutorial, 10 (4), 78-93

[2] Hu, Y. & Johnson, D.B. (2004). Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks. Proc. ACM SASN'04.

[3] Hu, Y.-C., Johnson, D.B. & Perrig, A. (2002a). Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Proceedings of Mobicom'02.

[4] Hu, Y., Perrig, A., & Johnson, D. (2002c). Packet Leashes: A Defense against Wormhole Attacks in Wire-less Networks. Proceedings of INFOCOM, IEEE

[5] Johnson, D., Hu, Y., & Malz, D. (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. IETF, Request for Comments (RFC) 4728

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

[7] Singh, U. (2011). Secure Routing Protocol in Mobile Ad Hoc Networks – A Survey and Taxonomy. Inter-national Journal of Reviews in Computing, 7 (2), 9-17. Retrieved

December 10, 2011 from http://www.ijric.org/volumes/Vol7/Vol7No2.pdf

[8] Yi, S, Naldurg, P., & Kravets, R. (2001). Security-Aware Ad hoc Routing for Wireless Networks. Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001

[9] Zapata, M.G. & Asokan, N. (2002). Secure Ad ho c On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, 3 (6), 106-107

Author Profile

Shwetha T.R, Completed B.E in Computer Science and Engineering at Nadgir institute of technology In Bangalore, Karnataka and currently pursuing the M.Tech degree in Computer Science and Engineering from East West institute of technology, Bangalore, Karnataka.

Prof Dr Arun Biradar, Currently working as HOD in computer science and engineering at East West institute of technology, Bangalore. He has more than 18 years of experience in teaching field. He is guiding M.tech students in the area of Computer Networks, Wireless Networks. His professional activities are Chairman Indian Society for Technical Education (ISTE), Karnataka Section Board of Examiner (BOE) Member, VTU, Belgaum and Served as managing committee member ISTE Karnataka