International Journal of Research in Advent Technology, Vol.5, No.10, October 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Survey on Secure Routing Protocols in MANETs

Mr. Sachin Korde, Dr. M. V. Sarode, Dr. V. M. Thakre
PhD Scholar[1], *Head of Department*[2, 3]
SGBAU, Amravati[1]
Government Polytechnic, Yavatmal[2]
SGBAU, Amravati[3]
sachin.kprde211@gmail.com[1]
mvsarode2013@gmail.com[2]

Abstract-: Mobile ad hoc networking (MANET) is gradually emerging in imitation of stand very important into the growth concerning wireless technology. This is expected after provide a extent over flexible purposes in accordance with mobile and nomadic users via potential over built-in identical architecture. The honest routing protocol is integral because better conversation within MANET. One of the current dependable 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 solely within nodes that wants to communicate. There are a number of safety problems in imitation of be considered within that protocol. In order after provide security for AODV protocol, Secure Ad Hoc On-Demand Vector Routing (SAODV) can be used. This order gives an overview over a number impervious routing protocols by way of offering their characteristics and performance along with their respective merits then drawbacks. For tightly closed protocol, digital signature, hash chains, etc., perform remain used of routing. This paper surveys over more than a few techniques handy for securing the mobile ad hoc network.

Keywords: Routing protocols, Security, MANET, attacks.

1. INTRODUCTION

Wireless Network is growing new technology in this modern era that will allow users to access services and information electronically, irrespective of their geographic positions. Wireless Networks are basically divided into two broad categories-Infrastructure Networks and Infrastructure less (ad hoc) networks. Infrastructure network has fixed and wired gateways. Whereas in the case of wireless network, there is no need of any type of wire. In Infrastructure Networks a mobile host interacts with a bridge in the network called base station within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range in one base station, it connects with new base station and start communicating through it. This situation is called Handoff. Next recent advancement Bluetooth introduced a fresh type of wireless system which is frequently known as mobile Ad hoc networks. MANET is self configuring network of mobile routers and associated hosts connected by wireless links.

Participating nodes acts as routers which are free to move randomly and manage themselves arbitrarily & thus the wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger internet. Hence the topology of the network is much more dynamic and the changes are often unpredictable oppose to the internet which is a wired network. In MANETs with each node acting as a router and dynamically changing topology the availability is not always guaranteed. It is also not guaranteed that the path between two nodes would be free of malicious nodes. The wireless links between nodes are highly susceptible to link attacks (passive eavesdropping, active interfering, etc). Stringent resource constrains in MANETs may also affect the quality of security. At the time of excessive computations is required to perform some encryption and decryption acts. The vulnerabilities and characteristic make a case to build a security solution, which provides security services like authentication, confidentiality, integrity, non-repudiation and availability. In order to achieve the goal which we need a mechanism that provides security in each layer of the protocol. [16], [17] Protection of MANETs can be divided into two categories, such as protection of the routing functionality (secure ad hoc routing) and protection of the data in transmission (secure packet forwarding). The way of approaching the MANETs protection can also be divided into two categories, such as proactive and reactive. Proactive approach attempts to prevent an attacker from launching

attacks, through cryptographic techniques. In reactive approach it seeks to detect threat and react accordingly. [16] The main objective of this paper is to give an overview of secure routing protocols, security analysis.

2. SECURITY ASPECTS OF MANETS

Some well-known Mobile Ad Hoc network applications are:

Collaborative Work: For some business environments, the need for collaborative computing might be more important outside office environments than inside. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.

Crisis-Management Applications: By using Ad Hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.

Personal Area Networking and Bluetooth: A personal area Network (PAN) is a short-range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

There are five major security goals that are needed to maintain a reliable and secure Ad hoc network environment.

There are mainly as following:

Confidentiality of Data - keeps data secret (usually accomplished by encryption).

Integrity of Data - prevents data from being altered (usually accomplished by encryption).

Availability of Data- data should be available on request.

Authentication of Data - verification that the data or request came from a specific, valid sender.

3. THREATS IN MOBILE AD HOC NETWORKS

The Protocols in MANET are vulnerable to many different types of attacks. In this section, I would like to list different types of attacks that are possible in these networks [13].

1) Attacks Using Modification An attacker node may modify certain contents of the routing packet, thus propagating incorrect information in the network

2) Attacks Using Impersonation A malicious node may try to impersonate a node and send data on its behalf. This attack is generally used in combination with modification attack.

3) Attacks Using Fabrication An attacker may try to fabricate a false Route Error message, which may cause other nodes to remove a particular node from it routing table.

4) Black Hole An attacker may create a routing black hole, in which all packets are dropped. by sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them.

5) Gray Hole As a special case of a black hole, an attacker could create a gray hole, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets

6) Replay In replay attack, previously captured routing traffic is sent back into the network to target new routes.

7) Wormhole This attack requires two malicious nodes where one node captures routing traffic, and sends it to the other malicious node. Then, the second node can send back selective information to the network.

8) Blackmail Here, the attacker can fabricate a list to block nodes and inject it into the network. This attack targets routing protocols that block malicious nodes by sending a black list of offenders to legitimate nodes.

9) Denial of Service This attack has two types: a) Routing table overflow, and b) Sleep deprivation torture. In the first type, the attacker floods the network with bogus route creation packets in order to prevent the correct creation of routing information, and to consume resources of nodes.

In Sleep deprivation torture, the attacker sends diverse routing information to a specific node in order to make it consume its batteries because of the constant routing processing.

4. CRYPTOGRAHIC MECHANISM FOR ROUTING IN MOBILEAD HOC NETWORKS

Cryptographic mechanism [15] is the most common and reliable means to ensure security and is not specific to *ad hoc* wireless networks, but can be applied to any communication network. This is some of the main mechanism used in MANETs

- *Asymmetric cryptography:* It is also known as publickey cryptography. In public key cryptography, there is a pair of public/private keys. The private key is kept private, while the public key can be public to others. One of the earliest public-key cryptographic techniques, known as RSA. Digital signature, key management, and other techniques have been developed in public-key cryptography, such as the ElGamal cryptograph system, DSA, and elliptic curve cryptography.
- *Symmetric cryptography:* The encryption key is closely related to the decryption key in that they are identical in most cases. In practice, keys represent a

shared secret between two or more parties that can be used to maintain private communication. Usually the network can choose a shared secret key to encrypt and decrypt the message once two more parties use a public/private key pair to build trust in the handshake stages, which is more feasible and efficient from a computational standpoint than asymmetric key techniques.

- *HMAC message authentication code:* It is a type of message authentication code calculated using a hash function in combination with a secret key. It can also be used to make sure that the message sent unencrypted retains its original content by calculating the message HMAC using a secret key.

5. SECURITY ROUTING PROTOCOLS IN MANETs

i)ARAN

ARAN [1], [2] is stand for Authenticated Routing for Ad Hoc Networks. ARAN is a security scheme, which can apply to any on-demand routing protocol. ARAN is similar to SAODV in many points; both of them are based on digital signature and also both of them uses control messages. Routing operations of ARAN's are performed using three data structures: Route Discovery Packet (RDP), Reply message (REP) and error message (ERR). These messages have the same functionality of RREQ, RREP and RERR messages in SAODV. Each of these messages has secured by digital signatures. These messages use the forward path and the reverse path during the routing discovery process. The messages use certificate revocation for detecting expired public keys. By model checking the two most common execution scenarios of ARAN with the AVISPA Tool, we have discovered the following attacks:

• *route disruption*, which occurs when the intruder prevents a route from being discovered;

• *route diversion*, which occurs when the intruder does not prevent the establishment of routes, but it achieves that some established routes are diverted;

• *creation of incorrect routing state*, which occurs when the intruder jeopardizes the routing states in some nodes. These attacks can be implemented by relying on some *spoofing behavior* of the intruder. We have found two different kinds of spoofing attacks on ARAN. In the first case, the intruder assumes the identity of a node that has moved away from its initial position; the node remains connected to the rest of the network only because of the intruder. Due to the spoofing activity of the intruder, the node can become part of a routing path, although it is actually disconnected from the rest of the network. This malicious activity can clearly lead to a route-diversion attack as well as a creation-of-incorrect-routing-state attack, as routing tables would contain incorrect information. A different spoofing attack can be achieved by using a number of malicious nodes to immediately forward route requests towards the destination. In this manner, the intruder bypasses the nodes in the route path together with the cryptographic calculations of the protocol. This immediately leads to a route-disruption attack as well as a creation-of-incorrect-routing-state attack.

ii)SAODV

The SAODV[3] protocol provides security mechanisms based on non-invertible hash functions and public key cryptography use applied to the on-demand routing protocol AODV. The node authenticity is guaranteed through the knowledge of the public key in each node of the network. An underlying key distribution mechanism is supposed to exist in the network.

In SAODV, hash chains are applied for the hop count authentication so that each node, at every hop can verify that the hop count metric was not maliciously decreased. In order to protect the immutable field of routing messages, each node generating a message includes a digital signature generated through its private key. Two modalities for the working of the protocols can be observed are 1) Destination only reply and 2) Route cache reply.

It is important to observe how in the first mechanism is a signature and second id modality. SAODV is possible to note the asymmetry algorithm in the resource deployment during the verification and signature of RSA. SAODV uses a double signature mechanism to allow an intermediate node to reply to a route discovery request on behalf of destination in order to reduce the complexity and computational overhead of double signature. This kind of mechanism applied in SAODV would require a HELLO periodical messaging mechanism activation for neighbor updating. The applied approach avoids this issue not introducing particular computational overhead because nodes observations is local such as decisions to react to some selfish behavior. SAODV is applied to a well know routing protocol, in order to improve its performance and to offer more resilience to attack from malicious nodes authenticated by the network. A preventive approach based on a cryptographic mechanism and a reactive approach to direct the anomalous and malicious behavior of nodes is considered.

iii)SDSDV

SDSDV[4] protocol is based on the regular DSDV protocol. Within SDSDV, each node maintains two one way hash chains about each node in the network. Two

additional fields are AL field(alteration) and AC field (accumulation) are added to each entry of the update packets to carry the hash values. With proper use of the elements of the hash chains, the sequence number and the metric values on a route can be protected from being arbitrarily tampered. This security in the routing protocols is necessary in order to defend against hostile attacks. The major goal is to protect the sequence number and the metrics in each entry of an update from being arbitrarily changed. SDSDV postulates that each node in the network, including itself, with one used for guarding against the decreasing metric attack and the other for against increasing metric attack. When listing an entry in an update for itself, a node places its own id and the hash value used for AC field relating to itself of current sequence number and metric. When an intermediate node transfers an entry for a destination node, it places in the AL field the id and the hash value in AL field received from the neighbor from which it learned the route to that destination. When an intermediate node receives an entry, it verifies the hash values in AL and AC fields. If the entire values pass the verification, the node accepts the entry otherwise the entry is neglected.

iv)ARIADNE

Secure On-Demand Routing Protocol for Ad hoc Network, ARIADNE [5], [6] is also proposed to secure DSR. Similar to SRP, it requires pre-deployment of authentication keys between the source and destination. Ariadne provide three key sharing approaches corresponding to three Authentication methods: pair wise shared secret keys, TESLA keys; shared secrets between communicating nodes combined with broadcast authentication; and digital signature. Pair wise shared secret keys authenticate DSR routing messages by using secret key between each pair of nodes. This requires n(n-1)/2 keys for a network consisting of n nodes. Pair wise shared secret keys avoid need for synchronization. TESLA requires time synchronization which is difficult to achieve in MANET environments. Each node should have a hash chain; the authentic element of each hash chain should be distributed to all network nodes. Also digital signature requires pre-deployed asymmetric cryptography for the authentication process. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives. Our proposed distributed technique is based on the propagation speeds of requests and statistical profiling; they do not require network-wide synchronized clocks, do not impose any additional control packet overhead, and need only simple computations by the sources or destinations of connections.

v)ENDAIRA

EndairA[6],[7] is one of the most secure ones and provides several defense mechanisms against so many types of attacks. It also incorporates our novel tunneling prevention mechanism into this modified version of endairA to defend it against the tunnelling attack. The mechanism utilizes the delays between receiving and sending control packets of endairA computed locality by all intermediate nodes. It detailed security analysis shown that it can limit the adversary's, ability to launch undetected tunnelling attack to an acceptable level. Our proposal does not change the number of control packets involved in endairA and only modifies the RREP messages slightly. endairA achieves a great efficiently in bandwidth utilization and computation overhead. It prevents adversarial nodes from impersonation forging, deleting any node from the list by the RREP packets. One of the most important features of one proposed mechanism to defend endairA against tunnelling attack is that it is a cross-layer approach in which the MAC layer timing operation has been exploited in the network layer operation and signaling. The reason which makes it necessary to utilize a cross-layer approach is that more information about the channel conditions such as congestion, delay and number of transmission in the MAC layer. One proposal need accurate time synchronization between all communicating nodes and with the help of more accurate GPS disciplined clocks, this is a simply accessible requirements. It detailed security analysis of the proposed approach show that it will drastically decrease the possibility of launching undetected tunnelling attack against endairA.

vi)SOLSR

Secure Optimized Link State Routing [9], provide the security with the help of signature scheme. And the approach provides the authentication between the two nodes. For providing the signature the approach uses the two functions. First one is for signature and the second is for verification

1. Sign (node id, key, message) a signature for a message can be verified in a node using a function:
2. Verify (originator id, key, message, signature).

To prevent malicious nodes from injecting incorrect information into the OLSR network, the originator of each control generates an additional security element called signature message and transmitted with the control message. A timestamp is associated with each signature in order to estimate message freshness. Thus, upon receiving the control message, a node can determine if the message originates from a trusted node, or if message integrity is preserved. Signatures are separate entities from OLSR control traffic: while OLSR control messages perform the purpose of acquiring and distributing topological information, signatures serve to validate information origin or integrity.

To compute a signature corresponding to a control message, the following protocol is used:

1. the node creates the control message;
2. the node retrieves the current time, and writes it in the Timestamp field;
3. the node computes the signature, and writes it in the Signature field;
4. the node puts the SIGNATURE message and the control message in the packet, in this exact order.

Then, the node sends the packet, or repeats the protocol for another control message before sending the packet.

vii)SEAR

A novel secure and energy aware (SEAR)[8] routing protocol to address these two issues concurrently through balanced energy consumption and probabilistic random walking. SEAR is designed with two configurable parameters, energy balance control (EBC) and security level. EBC is used to enforce energy balance and increase the lifetime. Security level is designed to determine the probabilistic distribution of the random walking that provides routing security. The security level can be defined by the message source on a message level, or on a system level.

SEAR algorithm consists of two methods for packet forwarding: shortest path forwarding based on the geographical information, and random forwarding, which is used to create routing unpredictability for source privacy and jamming prevention. As described in the introduction, we are interested in routing with energy balance, SEAR also has the flexibility to provide routing security and source privacy

5. CONCLUSION

Mobile adhoc network have been increase their vulnerability to attacks. This paper have discussed and presented various issues such as security attacks and threats can cause vulnerability in MANETs. It has been analyzed security mechanisms of various existing routing protocols in MANETs, which implements against various types of external attacks detect malicious behavior and provide a safer environment, with the secure routing can be successful authenticated and the malicious nodes can be identified. The summary report of the security issues, security attacks and surveyed completely secure mechanisms for MANETs have been presented.

REFERENCES

[1] Royer, E. (2002). A secure routing protocol for ad hoc networks. Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, 78{87. ISSN 1092-1648.

[2] Ahmed, Asma, et al. "MANET Security Schemes."

[3] De Rango, Floriano. "Improving SAODV protocol with trust levels management, IDM and incentive cooperation in MANET." Wireless Telecommunications Symposium, 2009. WTS 2009. IEEE, 2009.

[4] Wang, Jyu-Wei, Hsing-Chung Chen, and Yi-Ping Lin. "A Secure DSDV Routing Protocol for Ad Hoc Mobile Networks." INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on. IEEE, 2009.

[5] Hu, Y.-C., Perrig, A. and Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks.

[6] Benetti, Davide, Massimo Merro, and Luca Vigano. "Model checking ad hoc network routing protocols: Aran vs. \ endaira." Software Engineering and Formal Methods (SEFM), 2010 8th IEEE International Conference on. IEEE, 2010.

[7] Fanaei, Mohammad, Mehdi Berenjkoub, and Ali Fanian. "Resistant TIK-Based endairA Against the Tunneling Attack." Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on. Vol. 2. IEEE, 2008.

[8] Tang, Di, Tingting Jiang, and Jian Ren. "Secure and energy aware routing (sear) in wireless sensor networks." Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. IEEE, 2010.

[9] Guirguis, Shawkat K., and Youssef A. Othman. "Simulation analysis of secure routing in Mobile Ad hoc networks." Simulation 1.9 (2012).

[10] Eric Lee , Security in Wireless Ad Hoc Networks , Science Academy Publisher, United Kingdom , Vol. 1, No. 1, March 2011.

[11] Celia Li1, Zhuang Wang, Cungang Yang ,Secure Routing for Wireless Mesh Networks , International Journal of Network Security, Vol.12, No.3, May 2011
[12] J.Viji Gripsy , Dr. Anna Saro Vijendran ,A Survey on Security Analysis of Routing rotocols Global Journals Inc. (USA) , Volume ssue Version 1.0 April 2011
[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in ireless ad hoc network routing protocols.In Proceedings of the 2003 ACM Workshop on Wireless security, pages30–40, ACM Press, 2003.
[14] Ashwani Kumar, A survey on routing protocols for wireless sensor networks , IJAER , Vol.No.I, Issue No.2, February 2011.
[15] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[16] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.
[17] A.Weimerskirch and G.Thonet, "Distributed Light-Weight Authentication Model for Ad-hoc Networks," Lecture Notes In Computer Science; Vol. 2288, pp. 341-354, 2001.
[18] PM Jawandhiya, MM Ghonge, MS Ali, JS Deshpande, "A survey of mobile ad hoc network attacks", International Journal of Engineering Science and Technology(IJEST), 0975–5462
[19] MM Ghonge, PM Jawandhiya, "A Modified Grayhole Attack Detection Technique in Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer Science, 0976 – 5697
[20] MM Ghonge, PM Jawandhiya, MS Ali, "Countermeasures of network layer attacks in MANETs", IJCA Special Issue on "Network Security and Cryptography" NSC, 0975–8887
[21] M Ghonge, SU Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, 2277-128X
[22] SG Gupta, MM Ghonge, PD Thakare, PM Jawandhiya, "Open-source network simulation tools: An overview", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 2278 – 1323.