Review of applicability of G.A. in MANET

Renu Saini(Student, M.Tech CSE), Er. Amandeep Chhabra(A.P, CSE Deptt.)
GIMT, Kanipla, Kurukshetra, India

Abstract - Mobile Ad hoc Networks (MANETS) are transient, infrastructure less networks of mobile nodes, connected through wireless links, without any fixed infrastructure or supervisory management. Due to the self-configuring nature of these networks, the topology is highly dynamic in nature. This makes the Ad Hoc Routing environment in MANETs highly vulnerable to serious security issues. In this paper, we review the common security threats and attacks and summarize these solutions for applicability of G.A. in MANET. The survey provides the best possible methods which are used previously and help us to have new approaches to handle various issues.

Keywords - *MANET; Security attacks; Routing; G.A.; Network Security Solutions*

I. INTRODUCTION

An ad-hoc network is a collection of wireless mobile nodes forming a temporary network without assistance of any fixed infrastructure or centralized administrative control. Mobile Ad-hoc networks are self-configuring and self-organizing multi node wireless networks [1,5,6]. Each node in these ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its wireless range only. Nodes communicating, usually share the wireless media; as they transmit and get signals at the same frequencies, and follow the same wireless configuration. If the destination node is not present in the transmission range of the source node, the source node take help of the other nodes which will work as intermediate nodes in order to communicate with the destination node by relaying the messages hop by hop. Mobile wireless networks are open to various attacks, such as information and packet security attacks than fixed wired networks. Securing wireless ad hoc networks is particularly more difficult for many of the following reasons such as: vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology. The wireless channel is accessible to both authorized network users (normal behaving nodes) 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 not following the protocol specifications. The nodes are free to move in any direction randomly and organize themselves arbitrarily. They can join or leave the network at any time. Due to the frequently changing environment 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.

II. RELATED WORK

Several researchers have proposed secure routing protocols. For example, Perlman proposed flooding NPBR, an on -demand protocol designed for wired networks that floods each packet through the network. Flooding NPBR allocates a fraction of the bandwidth along each link to each node, and uses digital signatures to authenticate all packets. Unfortunately, this protocol has high overhead in terms of the computational resources necessary for digital signature verification and in terms of its bandwidth requirements. Furthermore, estimating and guaranteeing available bandwidth in a wireless environment is difficult [1].

Mobile Ad Hoc Network (MANET) techniques are critical to the success of emerging modern warfare concepts and are required to support communications for mobile military platforms, including ships, aircrafts, and ground vehicles operating in a highly dynamic and mobile tactical communications network with no fixed infrastructure. Research in Mobile Ad Hoc Networking has increased dramatically over the last few years with significant progress in hardware architectures, media access and routing protocols. Most of the work has been in simulation and small-scale laboratory demonstrations due to the significant resources required to implement an actual network with sufficient nodes to fully exercise the capabilities of both the hardware and software [4].

Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols [2].

Security in mobile ad-hoc networks is hard to achieve due to dynamically changing and fully decentralized topology as well as vulnerability and scarcity of wireless link. The first research effort in this area focused on providing a distributed certification server or trusted body. These works try to achieve emulation of certification authority in a dynamic ad-hoc scenario using the concept of threshold cryptography. Zhou and Haas focus on a key management service where there is no central authentication server. Trust of a single certification authority is distributed to a set of nodes, which share the responsibility of key management service. Additionally, Kong et al. also proposed a security architecture that depends on certification with threshold secret sharing. Their focus is to increase service availability, localization of security failures, and scalability with the network size. Asokan and Ginzboorg

provide a mechanism for a password based authenticated key exchange. A local context is set up by exploiting the physical presence of people in room, which can be used for sharing of stronger keys. In a large-scale civilian ad-hoc network is envisioned where nodes join and leave dynamically and do not have any trust relationship in priory. A self-organizing public key infrastructure is proposed that is driven by user's perception on 'trust' about others without depending on any certificate authority [8].

A client-server protocol that prevents ARP spoofing by automatically configuring static ARP entries was designed. The protocol works in both static, DHCP, wireless and MANET networks. Moreover, it can work in large-scale networks without any overhead on the administrator. In addition, the technique doesn't require special hardware to be deployed, as any host can work as ARP server [3].

Although security has long been an active research topic in wire line networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed [9].

III. SECURITY ATTACKS

A. Types of attacks

The security attacks in mobile ad hoc network classify network attacks into two categories: passive attacks and active attacks [6]. 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 attacks. In active attack, a malicious node disrupts the normal functioning of the system by performing either external or internal attacks. An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET.

- Modification attacks
- Impersonation attacks
- Fabrication attacks
- Wormhole attacks

These attacks are summarized as follows:

- *Modification Attacks:* A modification attack [6] 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.
- *Impersonation/Spoofing Attacks:* In this type of attack (also known as spoofing) [3] a malicious node uses, for example, the IP address 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.
- *Fabrication:* The main purpose of fabrication attacks [6] 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.
- *Wormhole Attacks:* A wormhole [5,6] 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
- *Selfish Attacks:* 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 [5,6] node also happens to be the only communication link between two MANET endpoints, communications between these endpoints will become unavailable.

B. 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. Due to the dominant status of reactive routing protocols for MANETs, most security research has tended to give attention to these protocols.

IV. 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 is a cryptographically protected version of QoS Route Discovery. SQoS Route Discovery relies entirely on symmetric cryptography.

B. Ariadne

Ariadne [1](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:

- Authentication of routing messages
- 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 [2], while AODV discovers the shortest path between two nodes. SAR can discover a path with desired security attributes [11]. 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 [12] 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 up to 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 [3] 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 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 [13] 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 the 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.

V. USING G.A. IN MANET

With the advancement in the technology of ad-hoc networks, several new routing protocols are designed for route maintenance and discovery.Genetic Algorithms which exist can provide solution for multi constrained problems related ot QoS. A new modified G.A. based routing protocol not only provides solutions to some problems but is well suited for the unique characterstics of MANET like dynamically varying network topology, lack of concrete state information, shared radio channel, limited resources access, hidden problems realated to terminal etc.

VI. 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 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. Further research needs to be undertaken both 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 single currently proposed routing protocol provides protection against all forms of routing attacks in MANETs.

VII. REFERENCES

[1] Y.C. Hu, A. Perrig and D.B. Johnson, "Ariadne: A secure on-demand routing protocol for wireless ad hoc networks", Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom 2002) (September 2002) pp. 12–23

[2] 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

[3] Shradha Shukla Indresh Yadav, "An Innovative Method for Detection and Prevention Against ARP Spoofing in MANET", International Journal of Computer Science and Information Technology & Security (IJCSITS),Vol. 5, No1, February 2015.

[4] Rich Folio, J. Bibb Cain and Sastri Kota, "Challenges in the Verification of Mobile Ad Hoc Networking Systems", International Journal of Wireless Information Networks, Vol. 14, No. 2, June 2007.

[5] Dr Karim KONATE, GAYE Abdourahime, "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", IEEE computer society (2011).

[6] Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[7] Thiyam Romila Devi, Rameswari Biswal, Vikram Kumar, Abhishek Jena, "IMPLEMENTATION OF DYNAMIC SOURCE ROUTING (DSR) IN MOBILE AD HOC NETWORK (MANET)", International Journal of Research in Engineering and Technology.

[8] Krishna Paul, Dirk Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks".

[9] Rakesh Kumar, Jha Suresh V. Limkar, Dr. Upena D. Dalal, "A Performance Comparison of Routing Protocols(DSR and TORA) for Security Issue In MANET(Mobile Ad Hoc Networks)", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[10] http://citeseerx.ist.psu.edu/showciting?cid=595103

[11] http://www.123seminarsonly.com/SeminarReports/026/49319701-Adhoc-networkSecurity-Survey.doc

[12] http://www.slideshare.net/kesanisruthi2000/ad-hoc.doc

[13] http://www.ukessays.com/essays/computer-science/security-issues-in-mobile-ad-hoc networks-computer-science-essay.php

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

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

Renu Saini, student of MTech.(CSE) at "Geeta Institute of Technology and Management", Kanipla, Kurukshetra.