A Survey on Security Issues in Routing in MANETS

C Sreedhar[#1], Varun Varma Sangaraju[*2]
[#]*Dept. of CSE, GPREC, Kurnool.*
[*]*Dept. Of CSE, Sathyabama University, Chennai.*

Abstract**—** Mobile Ad-hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. A MANET is a type of ad-hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks to accommodate the changing topology special routing algorithms are needed. There is no single protocol that fits all networks perfectly. The protocols have to be chosen according to network characteristics, such as density, size and the mobility of the nodes. In this paper, we make an attempt to address the various security issues and various attacks and challenges faced by the routing protocols in MANETs. There is still ongoing research on mobile ad-hoc networks and the research may lead to even better protocols and will probably face new challenges. Current goal of this paper is to find out the security issues and challenges of routing in MANETs.

Keywords**—** MANETs, Routing Protocols, Security.

I. Introduction

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. In a MANET, all the nodes co-operate amongst each other to forward the packets in the network and hence, each node is effectively a router. Thus one of the most important issues is routing. This paper focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad-hoc networks are described.

(a) *Distributed network:* A MANET can be considered as a distributed wireless network without any fixed infrastructure. By distributed, it is meant that there is no centralized server to maintain the state of the clients, similar to peer-to-peer (P2P) networks.

(b) *Dynamic topology:* The nodes are free to move arbitrarily with different speeds, thus the network topology may change randomly and unpredictable times.

(c) *Energy constraint:* Some or all of the nodes in an ad-hoc network may rely on batteries or other exhaustible means of sources of energy. For these nodes, the most important system design optimization criteria may be energy conservation.

(d) *Addressing scheme:* The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology entails a ubiquitous addressing scheme, which avoids any duplicate addresses. Mobile IP is currently being used in cellular networks where a base station handles all the node addressing. However, such a scheme doesn't apply to ad hoc networks due to their decentralized nature.

(e) *Limited Bandwidth:* Wireless links continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communications – after accounting for the effects of multiple access, fading, noise and interference conditions.

(f) *Security:* Mobile wireless networks are generally more prone to physical security threats than fixed wired networks. The increased possibility of eavesdropping, spoofing and minimization of denial-of-service type attacks should be carefully considered.

Security is the primary concern in wired or wireless networks [19]. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireline 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. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc [1]. Several attack scenarios have been proposed in the literature [20]. Therefore, mechanisms and protocols have to be developed to secure MANETs. This especially becomes relevant for a commercial use of this technology.

Because of the changing topology special routing protocols have been proposed to face the routing problem in MANETs. Since routing is a basic service in such a network, which is a prerequisite for other services, it has to be reliable and trustworthy. Otherwise no dependable applications can be provided over the MANET which brings up the need for secure routing protocols. A secure routing protocol has to be able to identify trustworthy nodes and find a reliable and trustworthy route from sender to destination node. In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes that are within each other's radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave and join the network and routes need to be updated frequently due to the dynamic network topology.

II. Issues in Routing Protocols in MANETs

At the highest level, the security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. *Authentication* is the verification of claims about the identity of a source of information. *Confidentiality* means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. *Integrity* means that the information is not modified or corrupted by unauthorized users or by the environment. *Availability* refers to the ability of the network to provide services as required. Denial of Service (DoS) attacks has become one of the most severe problems for network communication. In a military environment, a successful DoS attack is an extreme threat. Lastly, *non-repudiation* ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes. The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks. *Table 1* gives a few examples of attacks at each layer. Some attacks could occur in any layer of the network protocol stack, e.g. jamming at physical layer, hello flood at network layer, and SYN flood at transport layer are all DoS attacks. Because new routing protocols introduce new forms of attacks on MANETs, we mainly focus on network layer attacks.

Each of these attacks has to be addressed by a novel research which analyses insider attacks against AODV [4]. Achieving these goals depends on the capabilities of the adversary. The main factors affecting the performance of an attack are identified below

Computational power: This clearly affects the ability of an attacker to compromise a network. Such power need not be localized to the attached network – eavesdropped traffic can be relayed back to high performance super-computing networks for analysis.

Deployment capability: Adversary distribution may range from a single node to a pervasive carpet of smart counter-dust, with a consequent variation in attack capabilities [5]. This sort of distinction may affect the ability to eavesdrop, to jam a network effectively, and to escape destruction.

TABLE I
Attacks on Protocol Stacks

Layer	Attacks
Application Layer	Data Corruption, Viruses and Worms
Transport Layer	TCP/UDP SYN Flood
Network Layer	Hello Flood, Black hole
Data Link Layer	Monitoring, Traffic Analysis
Physical Layer	Eavesdropping, Active Interference

Location control: The location of adversary nodes has may have a clear impact on what the adversary can do. An adversary may be restricted to placing attack nodes at the geographical boundary of an enemy network, may deploy specific nodes, or may have the ability post facto to create a pervasive carpet of smart dust.

Mobility: Mobility generally brings an increase in power. On the other hand, mobility may prevent an attacker from continually targeting one specific victim. For example, a node on the move might not receive all falsified routing packets initiated by the attacker. In [6] Sun et al defined this phenomenon as being a "partial victim". Moreover they have stated that even if it reduces the damage caused by the attacker, it makes detection more difficult since the symptoms of an attack and those arising due to the dynamic nature of the network are difficult to distinguish. In conclusion, the impact of mobility on detection is a complex matter.

Degree of physical access including node capture ability and ability to carry out physical deconstruction, given the agile nature of MANETs determining an applicable adversary model is difficult. However, systems can be evaluated against a range of representative threat models

III. Security Threats For Routing Protocols in MANETs

MANETs are networks with no fixed infrastructure and network functions are carried out by all available nodes, which are highly mobile and have constrained power resources [10]. Consequently, MANET has increased sensitivity to node misbehavior [7] [8] [9]. There are two sources of attacks related to node misbehavior in MANETs [11]. The first is *external* *attacker*, in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load. The second is *internal attack*, which comes from the compromised nodes inside the network. Since compromised nodes can be authenticated, internal attacks are usually much harder to detect and can create severe damage. MANETs suffer from all the vulnerabilities that their wired counterparts encountered. An adversary may launch various attacks ranging from passive eavesdropping to active interference such as packet modification and fabrication, traffic jamming, denial-of-service (DoS), message reply and various other attacks [2].

Misbehave nodes in mobile ad hoc networks are classified into two types: *faulty/malicious nodes* and *selfish nodes* [12]. *Faulty nodes* refer to the nodes that are faulty and cannot follow a protocol, and *malicious nodes* are intentionally malicious and try to attack the network. The security problem caused by *faulty/malicious nodes* is extremely important in security sensitive applications. *Selfish nodes* are economically rational nodes whose objective is to maximize their own welfare. They will be the dominant type of nodes in a civilian ad hoc network. Although *selfish nodes* do not intend to attack the network, such selfish behaviors are also very harmful to mobile ad hoc network, which is highly dependent on the cooperation of all available nodes [12]. Although *passive* (eavesdropping) *attacks* are also possible in mobile ad hoc networks, they can easily be controlled by using cryptographic mechanisms. A*ctive attacks*, which are more damaging, cannot be defended by only applying cryptography mechanisms.

The goal of an active attack is to disrupt the proper function of the network. This may be achieved by several ways, some of the most common attacks are [13] [14]:

- Denial of service:
  - ○ Route Disruption (RD): breaking down an existing route or preventing a new route from being established.
  - ○ Direct Denial of Service (DDoS): preventing a given node from communicating with any other node in the network.
  - ○ Resource Consumption (RC): consuming the communication bandwidth in the network or resource at individual node.
- Route Invasion (RI): an attacker adds itself into a route between two nodes and takes control of the route.

Exploits against mobile ad hoc network routing protocols can be classified into modification, fabrication, tunneling attack, denial of service attack, invisible node attack, Sybil attack, rushing attack and non-cooperation.

A. Modification

Malicious nodes can modify the protocol fields of messages passed among nodes. Such attacks compromise the integrity of routing computation. By altering routing information, an attacker can cause network traffic to be dropped, redirected to a different destination or take a long route to the destination increasing communication delays [15]. Using AODV as an example, a malicious node can either increase the *broadcast_id in* RREQ to make the faked RREQ message acceptable, or it can decrease the *hop_cnt* to update other nodes' reverse routing tables. In the network illustrated in Figure 1, a malicious node M can increase the chances it is included on a newly created route from source node *S* to destination node *D* by consistently advertising to *A* a shorter route to *D* than that *B* advertises.

B. Fabrication

The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted.

C. Tunnelling Attack

Tunneling attack is also called wormhole attack. In a tunneling attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers [16].

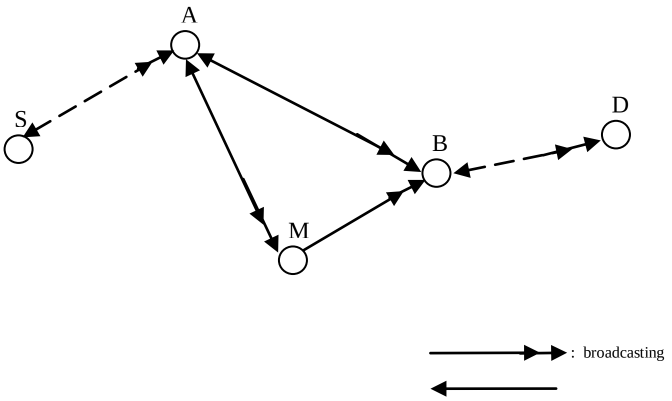

Fig. 1 Modification Attack

D. Wormhole Attack

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols.

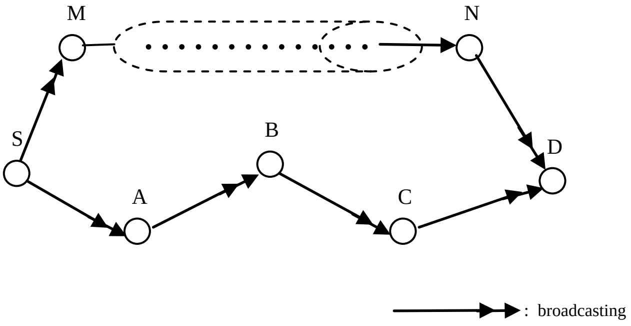

Fig. 2 Tunneling Attack

In Figure 2, M receivers RREQ, and tunnels it to N. When N receives the RREQ, it forwards the RREQ to D as if it had traveled S, M and N. N also tunnels the RREP back to M. By doing this, M, N falsely claim a path between them and fool S to choose the path through M, N (because it has shorter path length). The tunnel between the attackers is actually faster than links between legitimate nodes, so the tunneled packet arrives sooner than packets through other route. Therefore, the attackers are more likely to be included in a route by claiming a shorter path and then they can take control of the route.

E. DoS Attack

This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.

F. Invisible Node Attack

Invisible node attack is possible on DSR routing protocol. In this kind of attack, the malicious node does not append its IP address and thus it becomes difficult to find out this kind of attack. A malicious node M becomes invisible on the path and hence the path from the source to the destination could not be achieved.

G. Sybil Attack

Sybil attack refers to represent multiple identities. If a malicious node colludes and shares their secret keys then this kind of attack is known as Sybil attack. In MANETs, where the functionality relies on the trust of each node, the Sybil attack is very harmful. By "being in more than one place at once", the Sybil attack disrupts geographic and multi-path routing protocols. In a mobile ad hoc network that uses multi-path routing, the possibility of choosing a path that contains a malicious node M will be largely increased.

The following table describes the summary of the various issues in securing routing protocols in MANETS.

TABLE II
ATTACKS ON PROTOCOL STACKS

Type of attacks	Description	Results
Modification	Modify the routing message	DoS, take control of the route
Fabrication	Generate false routing messages	DoS, take control of the route
Tunneling attack	Colluding, take advantage of "tunnels"	Take control of the route
DoS attack	Floods irrelevant data, resource consuming	DoS
Invisible node attack	Malicious node becomes "invisible"	DoS
Sybil attack	Colluding, forging of multiple identities	DoS, take control of the route
Rushing attack	Rushing routing message	Take control of the route
Non-cooperation	Not participate, selfish behavior	DoS, take control of the route

H. Rushing Attack

During the process of route discovery, only the first received route request packet (RREQ) is processed. If the RREQ forwarded by an attacker is the first to reach the destination node, then the route discovered will include the hop through the attacker [39]. Thus, an attacker that can forward Route Request packets more quickly than legitimate nodes can increase the probability of being included in the discovered route. In a rushing attack, the adversary succeeds in fooling the source into believing that a route is short, by relaying packets much faster through nodes under his control. An attacker can achieve faster transit by transmitting at a higher wireless transmission power level or may employ a wired tunnel which is much faster than wireless forwarding.

I. Non Cooperation

In mobile ad hoc networks, the resource of a mobile node is restricted. In order to get the most benefit, a mobile node may behave selfishly to save energy for itself; it may not participate in routing or may not forward packets for other nodes. This kind of node misbehavior caused by lack of cooperation is called *node selfishness*. A selfish node differs from a malicious node for it does not intend to damage other nodes with active attacks, but the damage selfish behaviors cause to the mobile ad hoc network cannot be underestimated.

IV. Conclusions

In this paper, we have analyzed the security threats an ad-hoc network faces. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats.

References

[1] C.E.Perkins and E.M.Royer, “Ad-Hoc on Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2] C Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath, “Potential Security Attacks on Wireless Networks and their Countermeasures”, In IJCSIT, Vol.02, No. 05. .

[3] Perkins C., Belding-Royer E., Das S., “RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing”, http://www.ietf.org/rfc/rfc3561.txt, 2003.

[4] Ning P., Sun K., “How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols”, In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003.

[5] Chivers H., Clark J. A., “Smart dust, friend or foe?--Replacing identity with configuration trust”, Computer Networks 46(5), pp. 723-740, 2004.

[6] Sun B., Wu K., Pooch U.W., “Zone-Based Intrusion Detection for Mobile Ad Hoc Networks”, Int. Journal of Ad Hoc and Sensor Wireless Networks, vol.2 , no. 3, 2003.

[7] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens, An On-Demand Secure Routing Protocol Resilent to Byzantine Failures, In *ACM Workshop on Wireless Security (WiSe)*, Atlanta, Georgia, September 28 2002.

[8] Pietro Michiardi and Refik Molva, Ad hoc networks security , In *ST Journal of System Research*, Volume 4, March 2003

[9] Pietro Michiardi and Refik Molva .Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks **,** *European Wireless Conference*, 2002

[10] L.Zhou and Z. hass. Securing ad hoc networks. *IEEE Network*. 13(6):24-30, November/December 1999.

[11] Sheng Zhong, Jiang Chen, and Yang Richard Yang, Sprite: A simple, Cheat-proof, Credit-based System for Mobile Ad hoc *Networks*, in *Proceedings of IEEE Infocom '03*, San Francisco, CA, April 2003.

[12] Pietro Michiardi and Refik Molva .Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks **,** *European Wireless Conference*, 2002 .

[13] Peng Ning, Kun Sun, How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols, in *Proceedings of the 4th Annual IEEE Information Assurance Workshop*, pages 60-67, West Point, June 2003.

[14] Shahan Yang and John S. Baras, Modeling Vulnerabilities of Ad Hoc Routing Protocols. *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)* October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[15] Y-C Hu, A. Perrig, D. B. Johnson, Ariadne : A secure On-Demand Routing Protocol for Ad Hoc Networks, in *proceedings of MOBICOM 2002.*

[16] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. A secure routing protocol for ad hoc networks. *Technical Report 01-37*, Department of Computer Science, University of Massachusetts, August 2001 .

[17] Peng Ning, Kun Sun, How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols, in *Proceedings of the 4th Annual IEEE Information Assurance Workshop*, pages 60-67, West Point, June 2003.

[18] Shahan Yang and John S. Baras, Modeling Vulnerabilities of Ad Hoc Routing Protocols. *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)* October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[19] C Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath, “ Performance Analysis Secure Routing Protocols in Mobile Ad-Hoc Networks”, In IJCST, Vol.03, Issue 1.

[20] A. Martin, J. Smith, and M. Koethe, “A Platform Independent Model and Threat Analysis for Mobile Ad hoc Networks”, proc. of the 2007 Software Defined Radio Technical Conference, Denver, Colorado, Nov. 2007.