Routing and Security in Self Organizing Mobile Ad Hoc Networks (MANET): Challenges and Solutions

Ashish Patel
Department of Computer Engineering
SVM Institute of Technology
Bharuch, INDIA
adp_svmit@yahoo.co.in

Rutvij Jhaveri
Department of Computer Engineering
SVM Institute of Technology
Bharuch, INDIA
[2]rhj_svmit@yahoo.com

Abstract*:* **Ad hoc networks in general have to deal with a highly decentralized as well as a continuously changing topology due to the mobility of the nodes. MANET is not a new paradigm in wireless community. The technology is quite old but still practical implementation is difficult due to security and other problems. Since the ad hoc environment is very vulnerable to a multitude of different attacks, new methods of securing these network environments have to be developed. Mobile ad hoc networks or MANETs are supposed to play an important role in future military communication, natural disaster, isolated areas and many more. But while offering many advantages, the MANET technologies today are facing new security threats. Only one malicious node can be sufficient to distort operation in a MANET not using any security mechanism. Number of different algorithms and solution are available, but, realization of robust security architecture is impossible without proper understanding of possible threats and their consequences.**

Keywords: MANET, Intrusion Detection, Routing Protocols, Denial-of-Service

I. INTRODUCTION

Basically, the wireless ad hoc networks can be classified in static, mobile, or hybrid, based on the behavior of the nodes. In general, the mobile networks present more complexity than the static ones, because with mobility the arrangement of network is constantly changing, which imposes control challenges for communication. There are many applications for MANET's. These include personal area networking, cell phones, laptops, military operations etc. In addition they could prove useful in civilian environments as transportation networks, conference rooms, ships, and rescue operations as well as policing and firefighting. There are fundamental differences between the architecture of wired networks and wireless networks. First the available bandwidth is very less than that of wired networks. Second, all communication in a wireless network is broadcast. Third, there is a limited battery power. And finally, wireless links are much more error prone compared to wired links.

Wireless ad hoc networks require no base station and all the control and access tasks are distributed among nodes acting as peers. This makes them attractive in situations where there is no fixed infrastructure. However, the lack of centralized control imposes significant challenges for ad hoc network designers and there are many open problems, like delay over communication channel, organization and control of scattered nodes and power consumption need clarification. Also, the network modeling issue is a research challenge, and more complete and real models are necessary to help the analysis.

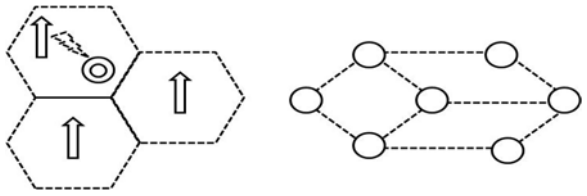

Figure 1: Cellular model VS ad-hoc model

Fig 1 shows the differences in cellular and adhoc model. The unique characteristics of MANETs pose a number of challenges to security design.

1. Open and sprinkled network architecture.

2. Dynamic network topology.
3. Shared wireless medium.
4. No proper defense mechanism.
5. Distribution of up-to-date location.

Ongoing research includes research and studies on various types of attacks on both civilian and tactical MANETs along with possibilities of attack detection using network and attack simulation tools. In addition to work on modeling and simulation, implementations and field trials for routing protocols and mechanisms for attack detection are also conducted, typically using handheld devices such as PDAs running the Linux operating system platform.

All ad-hoc networks share the following features. [13]

1. Not all nodes are within line of sight of each other of a base station. Thus, packets may have to be relayed several times over the multiple access channels.
2. Nodes can serve as sources, relays and destinations of data traffic.
3. Due to limited transmission range, mobility causes frequent changes in connectivity.

Protocols used in MANETs cannot rely on a centralized system to be functional. Known security protocols used in wired networks usually rely on a server. Hence, these protocols cannot directly be applied in the ad hoc environment. Either they have to be altered or new protocols or mechanisms have to be designed to introduce security within the decentralized MANET environment. Many different suggestions for security protocols in MANETs exist. Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding. Routing protocols assumes collaboration between nodes.

Protocols families:

1. Proactive: use messages to populate Routers
2. Reactive (o On-Demand): don't use Routers
3. Hybrid

There are many routing protocols proposed till date as per shown in fig 2, but most of the protocols lacks of security mechanisms.

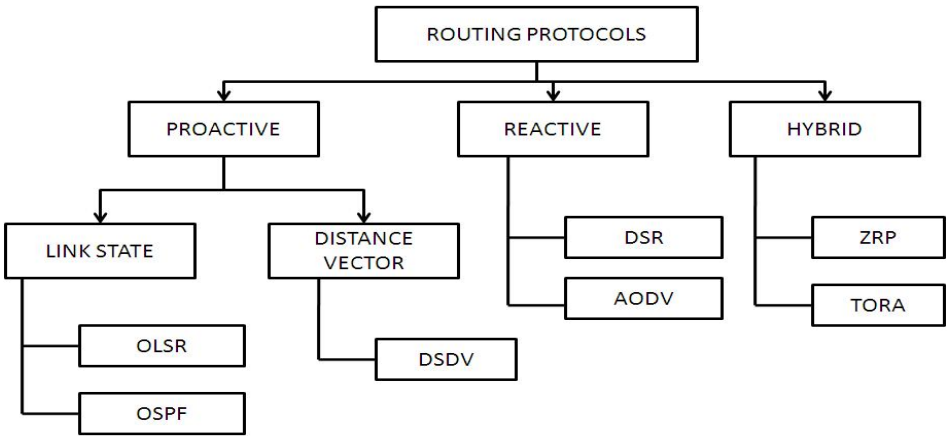

Figure 2: MANET Routing Protocols

Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

II. SECURITY ISSUES [3]

All attacks type of wired networks is possible in MANET. MANET has also several types of attacks, which are not available in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks. While considering the security issues, one has to think about the type of attack can be done on MANET. There are mainly two types of attack, passive attack and active attack [19]. Passive attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. First we should analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. We can then point out various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, we can find out several security schemes that can partly solve the security problems in the mobile ad hoc networks. [24]

A. Secure Multicasting

Multicast is a way to send messages to a group of recipients. This is in contrast with unicast, which is used to transmit a message to one recipient, and broadcast, which is used to transmit the message to all nodes in the network. Multicast has many applications, for instance, in audio and video conferencing, computer supported co-operative work (CSCW), distributed databases, video and audio distribution and finding network services.

B. Secure Routing

The protocols, data, and algorithms that compute paths through interconnected network devices are possibly the most vital, complex, and fragile components in the global information infrastructure. They are also the least protected. This article examines the current state of, and practical prospects for, security in IP routing infrastructures.

C. Privacy-aware Routing

It allows users to disclose minimum information possible while maintaining accountability. It allows privacy-aware secure user communication, while satisfying the above two capabilities simultaneously.

D. Group Membership Control

Due to the dynamic topology of MANETs to build optimal multicast trees and maintaining group membership a lot many control messages required. These overhead consume the mobile node resources like power and network resources like wireless links bandwidth that creates hurdle in implementing energy assurance and reduced overhead multicast protocol for Mobile Ad hoc Networks. [7]

E. Key Distribution

Secret communications with secret keys implies that only trusted parties should have copies of the secret key. That is, although secret keys can assure us of confidentiality, authentication of users and message integrity, in a global world we must be able to securely distribute keys at a distance in a timely manner. If security is to be maintained, key distribution must be as solid as the cryptographic method and be able to assure that only trusted parties have copies of the keys. Obviously, key distribution is a very big problem.

F. Intrusion detection

Intrusion detection and Response Systems Intrusion detection (ID) is a type of security management system for computers and networks as shown in fig 3. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

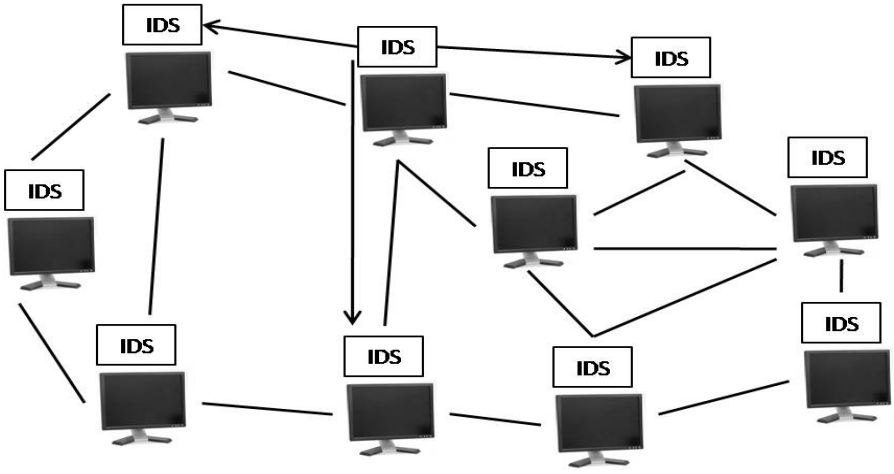

Figure 3: Intrusion Detection System (IDS) for MANET

III. SOLUTIONS

Many security solutions are given in Mobile Ad-Hoc Network. If we divide them in different areas then they can be listed as,

1. Prevent the fabrication, modification, and replay of routing messages by all classes of intruder.
2. Prevent the deletion of routing messages by subverted links and subverted routers.
3. Prevent the disclosure of routing messages by all classes of intruder.

Base on the above areas the main issues are discussed below.

A. Network Layer Security

Networking protocols are organized as a stack of responsibilities. For wireless networking, that stack is called the Wireless Application Protocol (WAP) stack. Within WAP, the Wireless Transport Layer Security (WTLS) Protocol is defined as the wireless equivalent of the Transport Layer Security (TLS) protocol for wired networks. [15, 16]

Like TLS, WTLS relies on a system of security certificates for authentication, backed up by encryption on data transfers. This encryption has to be negotiated at the point a connection is made. There are a number of different encryption algorithms at the protocol's disposal and the particular system to be used is negotiated between client and server as part of the WTLS procedures

B. Secure Ad Hoc Routing

Several routing protocols have been proposed for routing in ad hoc networks; however, until recently, security in such networks has not yet enjoyed much attention from the research community [8]. As a result, ad hoc network routing protocols that assume a trusted environment are highly vulnerable to attack; for example using the wormhole or rushing attacks, an adversary can paralyze ad hoc networks.

C. Secure Packet Forwarding

Routers have to decide what form packets should have when forwarded. A problem with today's Internet Protocol is that headers are relatively large. When payloads are small, header overhead can become prohibitive.

D. Link-Layer Security

The Link Layer is better known as the Data Link Layer. This term applies to the second level in the TCP/IP (Transmission Control Protocol/Internet Protocol) and OSI (Open Systems Interconnection) protocol stacks. The Data Link Layer is responsible for converting data into electronic pulses to be sent over a wire. Security on network transmission is usually implemented at the Transport Layer or the Application Layer. The IPSec protocol brings encryption to the Internet/Network Layer. Mobile communications are vulnerable to security breaches and so there is a greater need to push responsibility even further down the protocol stack. [22]

IV. AREAS OF RESEARCH

One big topic for research is security and the development of efficient security mechanisms. Since securing MANETs is a very challenging task, no final overall solution has been developed so far. The research areas include attack and intrusion detection for MANETs. In support of this, research on risk and attack analyses as well as formal and semi-formal modeling and simulations are also conducted. A second main area of research lies in the investigation and development of secure and reliable routing protocols for MANETs, particularly protocols capable of taking application-specific requirements into account [9]. Another area of specific interest lies in protocols which can include external sensor data and information such as geospatial positioning and topographical data into routing computations. Such considerations are also included in research into intrusion and attack detection as means for improving both node and network-wide situational awareness. [21]

V. CONCLUSION

Because this is a review paper, we have tried to address some common issues in mobile adhoc network. Importance of MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. Security is not a single layer issue but a multilayered issue. It requires a multi fence security solution that provides complete security spanning over the entire protocol stack. The Study of this important issue reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and management, secure architecture, intrusion detection and protection etc. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches [4]. The solution should comprise of all three components: prevention, detection and reaction. One necessary and sufficient condition is cooperation between nodes; The network performance severely degrade when a large percentage of node do not cooperate. So always there is a need to enforce collaboration between nodes.

REFERENCES

[1] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, “Security in mobile ad hoc networks: Challenges and solutions”. IEEE Wireless Communications. 11 (1), pp. 38-47, 2004.

[2] Wiki - http://en.wikipedia.org/wiki/Denial-of-service_attack

[3] B Sathish Babu Indo-UK Workshop on Ubiquitous Computing - 2005, Indian Institute Of Science, Bangalore.

[4] Giancarlo Pellegrino, "Security in Mobility", Mini Workshop on Security Framework 2006, Catania, December 12, 2006

[5] David B. Johnson, David A. Maltz - “Dynamic Source Routing in Ad Hoc Wireless Networks” - Mobile Computing edited by Tomasz Imielinski e Hank Korth, Kluwer Academic Publisher, 1996;

[6] Harald H.-J. Bongartz, Tobias Ginzler, Thomas Bachran, SEAMAN: A Security-Enabled Anonymous MANET Protocol, NATO Consultation

[7] Pariza Kamboj, Ashok.K.Sharma “Energy Efficient Multicast Routing Protocol for MANET with Minimum Control Overhead (EEMPMO)” IJCA Journal, Number 7 - Article 1, 2010

[8] Hu, Yih-Chun, and Adrian Perrig. "A Survey of Secure Wireless Ad Hoc Routing." In IEEE Security & Privacy, special issue on Making Wireless Work, 2(3):28-39, May/June 2004

[9] Peter Ebinger, “MANET Security Security in Mobile Ad-hoc Networks (MANETs)”, Department Security Technology, ", Fraunhofer-Institut für Graphische Datenverarbeitung IGD.

[10] M. Ramkumar, N. Memon, KPI: A Security Infrastructure for Trusted Devices, Pre-Conference. Workshop, 12th Annual Network and Distributed System Security Symposium, San Diego, California, 2 February 2005.

[11] David B. Johnson, David A. Maltz - “Dynamic Source Routing in Ad Hoc Wireless Networks” - Mobile Computing edited by Tomasz Imielinski e Hank Korth, Kluwer Academic Publisher, 1996;

[12] C. Perkins, E. Belding-Royer, S. Das RFC3561 - “Ad hoc On-demand Distance Vector” - http://tools.ietf.org/html/rfc3561

[13] The Network Simulator http://www.isi.edu/nsnam/ns

[14] L. Heberlein, G. Dias, et.al. “A network security monitor”. In Proceedings of the IEEE Symposium on Security and Privacy, pp. 296-304, 1990

[15] Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. In Mobile Computing and Networking, pages 189–199, 2001.

[16] P. Ramachandran and A. Yasinsac. Limitations of On Demand Secure Routing Protocols. Information Assurance Workshop, 2004. Proceedings from the FifthAnnual IEEE SMC, pages 52–59, 2004.

[17] M. G. Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In WiSE ’02: Proceedings of the ACM workshop on Wireless security, pages 1–10, New York, NY, USA, 2002. ACM Press.

[18] Y. Hu, A. Perrig, and D. Johnson. “Rushing attacks and defense in wireless ad hoc network routing protocols”. In Proceedings of ACM MobiCom Workshop - WiSe’03, 2003

[19] J. R. Douceur. “The sybil attack”. The 1st International Workshop on Peer-to-Peer Systems pp. 251–260, 2002.

[20] J. Hubaux, L. Buttya´n, S. Capkun, “The quest for security in mobile ad hoc networks.” The2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2001

[21] P. Papadimitratos, Z.J. Haas, E.G. Sirer, “Path set selection in mobile ad hoc networks”, The Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 1–11, 2002

[22] Debar, M. Dacier, and A.Wespi, “A Revised Taxonomy for Intrusion-Detection Systems”. Annales des Telecommunications, pp. 361-378, 2000

[23] A.J. Menezes, S.A. Vanstone, P.C. Van Oorschot, “Handbook of Applied Cryptography”. CRC Press, Inc., USA (2001).

[24] Wenjia Li and Anupam Joshi, “Security Issues in Mobile Ad Hoc Networks - A Survey”, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.