A Survey on Security Challenges in Routing Protocols and Schema in MANET

Muskan[1], Dr. Nitin Pandey[2]

[1] Student, Amity Institite of Information & Technology, Amity University, Noida, Uttar Pardsh, India
[2] Asst. Professor, Amity Institite of Information & Technology, Amity University, Noida, Uttar Pardsh, India

---

Abstract - ***A Mobile Ad hoc network (MANET) is a keen robotized dynamically circulation of wireless Mobile autonomous hubs they either join clearly or using halfway node(s) with no predefined infrastructure. In the event that there is no predefined infrastructure then networks get unprotected to number of attacks and security challenges become an important concern. The first section talks about brief introduction, features and routing protocol of MANET. The second section discuss about the vulnerabilities in MANET. MANET is a standout amongst the most vital fields for study, advancement and examination of remote networks. Mobile Ad Hoc Networks (MANETs) has turned into a standout amongst the frequent areas of exploration in view of the security Challenges it faces to related protocols. The third section talks about the security challenges in routing protocols in MANET. The last area examines Intrusion Detection Techniques (IDT), IDS structural planning and the conceptual model of IDS agents. MANET nodes are widely changing & joining the dynamic network. It is is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can get to be rogue and can get to be danger as these nodes have a place with the trusted zone. This challenge is overcome by assigning an impermanent id to every node.***

Key Words: *MANET, Securiy Goals, Schema, Challenges, IDT, Vulnerability*

1. INTRODUCTION

Network technology has ended up extremely significant viewpoint and has numerous impacts on individuals' life, for example, exchanging resources, data and information smoother and quicker. Wi-Fi, APN, Wi-MAX are the different networks which helps individuals to share resources, exchange related data and imperative information between distinctive sorts of devices the whole way across the world [1]. However, the same network technology and strategies have been utilized by individuals to hack and attack the network with developing information flow inbound and outbound in.

Mobile Ad hoc network (MANET) is a self forming arrangement of wireless mobile free nodes; they either join clear or using midway node(s) with no predefined framework. The unfixed infrastructures and routers have ability to move free anyplace with no restrictions. Mobile has antennas that gets and transmits data. Thus, self arranging networks joins' mobile wireless communications with high degree node adaptability, autonomy and portability [2] [3]. The users make utilization of numerous electronic platforms however which they can get to all the relative information and data at whatever point and wherever they are [2]. Likewise, MANET nodes can speak straightforwardly with different nodes inside the communications ranges; while nodes those are not in their communications reach use of intermediate road node(s) to communicate hence this arrangement of mobile networks can be represented to as MANET.

Table -1: Features of MANET[4]

Bandwidth-synthetic, variable capacity links	In MANET, remote connections have respectably lower limit than their hardwired real parts. In addition, the performed stream limit of remote interchanges in the wake of computing for the predominance of numerous access and impedance conditions.
Energy-synthetic operation	Sometimes a number of the nodes may rely on upon batteries implies for their energy.

Restricted physical security	MANETs are many times more attract to number of security dangers than are settled wired networks.
Self-forming	Nodes that come extremely close to one another can secure a network acquaintanceship without any pre-configuration or manual intercession.
Self-healing	Nodes can join or leave quickly without influencing operation of the remaining nodes.
No Infrastructure	In a wireless ad hoc network, mobile nodes structure their own particular network and basically turn into their Infrastructure.
Peer-to-Peer	Traditional networks normally help end frameworks working in customer server mode. In an ad hoc network, mobile nodes can impart and trade data without earlier arrangement and without dependence on concentrated assets.
Predominantly Wireless	Historically, networks have been basically wired and improved or reached out through remote access. The ad hoc environment is basically remote, yet could be stretched out to backing wired assets.
Highly dynamic	Mobile nodes are in nonstop movement, and ad hoc networking topologies are always showing signs of change.

The most accepted routing protocols used in MANET are:

1. Reactive Routing Protocols
2. Proactive Routing Protocols
3. Optimized Link State Routing Protocol (OLSR)
4. The Topology Broadcast Routing Protocols
5. Dynamic Source Routing Protocol (DSR)
6. Ad-hoc On-demand Distance Vector Routing Protocol (AODV)

This paper talks about the number of vulnerabilities that are inherited from the given features of MANET. Organization of paper has been done as takes after. The second section talks about the vulnerabilities in MANET. Because of the features of routing protocols, the security of MANET is developing as extraordinary test. The third area talks about the security challenges in steering conventions in Mobile Ad hoc network. The last area talks about Intrusion Detection Techniques (IDT), IDS structural planning and conceptual model of IDS agent. MANET nodes are broadly changing & joining the mobile network.

It is unrealistic to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can get to be rogue and can get to be danger as these nodes have a place with the trusted zone.

2. VULNERABILITIES OF MANETs

There are numerous important features of MANET which makes it well known, however vulnerability still emerges because of the inherent features of self-arrangement and re-development. A definite talk for the reasons is said underneath:

1. Lack of Secure Boundaries

Nodes inside MANET have no limitation for nodes to associate, join, detach and go in or outside of the network. Along these lines, the absence of security measures makes the MANET inclined to the attacks. The MANET is open to attack because of absence of firewall and network gateway [6].

2. Dynamic Topology

Since, nodes are changing & joining the mobile network. It is impractical to record the freed accomplished by node(s) in a dynamic network.. Some of these nodes can get to be rogue and can get to be danger as these nodes have a place with the trusted zone [10].

3. Inaccessibility of Centralized Management

There is no operation control focus i.e. brought together organization office, for MANET i.e. a name server, which prompts some defenseless challenges. Subsequently it gets to be hard to screen the activity in a significantly dynamic and extensive scale network [7]. This issue brings about breakdown and failure in transmitted data. Thus, nodes don't contribute in any security operations. An inadequacy of this type cause can hamper the general operations of the nodes association and disjoints [5][8][11].

4. Bounded Power Supply

The nodes depend totally on the battery as their energy supply procedure. This is a constrained type of force

supply. The failure talked about can exist in a spite second bringing on various challenges contrasted with the wired network [13].

5. Alterable Scalability

All things considered wired network scale is predefined when outlined and not change such all through the usage, however scale is changing each time in light of adaptability in MANET. There is no network to anticipate number of nodes in MANET. This infers that network needs scale all over at every one time in network [14].

3. SECURITY CHALLENGES IN ROUTING PROTOCOLS IN MANET

3.1 Attacks on Routing Protocols

Ad-hoc networks are more effortlessly challenged as opposed to other wired network. The challenged overwhelming on Ad- routing protocols are characterized as- Passive Attack are not ready to disturb the behavior of the protocol, yet uncover productive data by tuning into movement. Passive attacks in a general sense incorporate gaining essential routing information by sniffing about the network. Such attacks are customarily troublesome to place and in this way, guarding against such attacks is stupefied. Despite the way that it is unrealistic to perceive the accurate area of a node, one may be able to uncover data about the network topology, utilizing these attacks. An Active Attack, notwithstanding, pervades subjective groups and tries to madden the operation of the protocol remembering the completed goal to cutoff openness, get affirmation, or constrain in parcels bound to particular nodes. The target is in an expansive manner to draw in all groups to the attacker for challenges or to weaken the network. Such attacks could be set and the nodes may be perceived [15].

3.2 Attacks on MANETs

There are different types of attacks in MANETs; however most recognize attacks are [12]:

3.2.1 Eavesdropping Attacks

Eavesdropping is known as exposure attacks, commonly done by external or internal nodes and is uninvolved. The attacker's target of Eavesdropping is to separate show messages and procure some accommodating information about the network that is important all through the communication [9].

3.2.2 Denial of Service (DoS)

In DoS attacks, attackers endeavor to attack at the availability of organizations of the entire Mobile Ad hoc network. The attackers use the battery exhaustion routines and the radio adhering to perform Dos attacks to the Mobile Ad hoc network.

3.2.3 Dropping Attacks

In Mobile Ad hoc network nodes those are malicious nodes intentionally drops all the packets that are not headed for them. In dropping attack, malicious nodes expect to disturb the affiliation, while self absorbed nodes plan to protect their benefits. It diminishes the network execution by bringing on data packs to be transmitted yet again; new routes to the destination are to be found.

4. SECURITY SCHEMA IN MANETs

Intrusion Detection Techniques (IDT)

There are various difference between the wired network and the MANET, Intrusion detection system is initially settled in the wired network and has changed into the vital main security respond in due request with respect to the wired network, has furthermore gotten several contemplations from the investigators when they investigate the security respond in due request in regards to the MANET. In the going with, some conventional interruption recognition techniques in the mobile ad hoc networks in purposes of interest [16][17].

4.1. Intrusion Detection Techniques (IDT) in MANET

In this architecture (figure 1), every node in the MANETs takes an interest for the IDT process and response practices by recognizing tracks of intrusion lead regional standards and uninhibitedly, which are built by the intrinsic Intrusion Detection System operators. On the other hand, the nodes may offer their controlled results to everybody in this manner and join in a wide physical field. The coordinated effort in nodes usually happens when a node gets generally yet not sufficiently having affirmation to complete what kind of intrusion it interfaced to.

In the conceptual model, Main functional modules are:

1. Local data collection module, fundamentally deals with the information get-accumulation issue, the progressing survey information may begin from diverse radio resources.

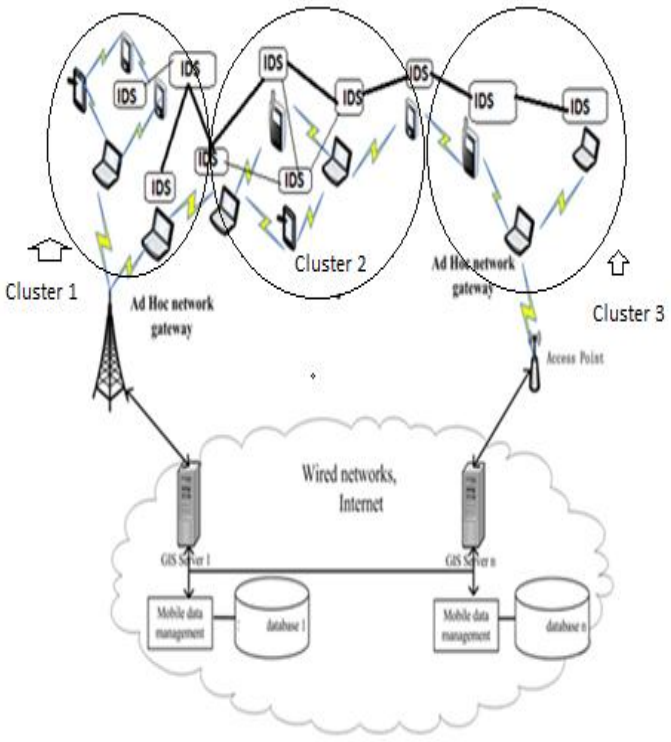

Figure 1 Intrusion Detection System for MANET [20]

2. Local detection engine inspects at the nearby information assembled by the neighborhood information gathering module and researches to weigh the irregularity demonstrated in the data.

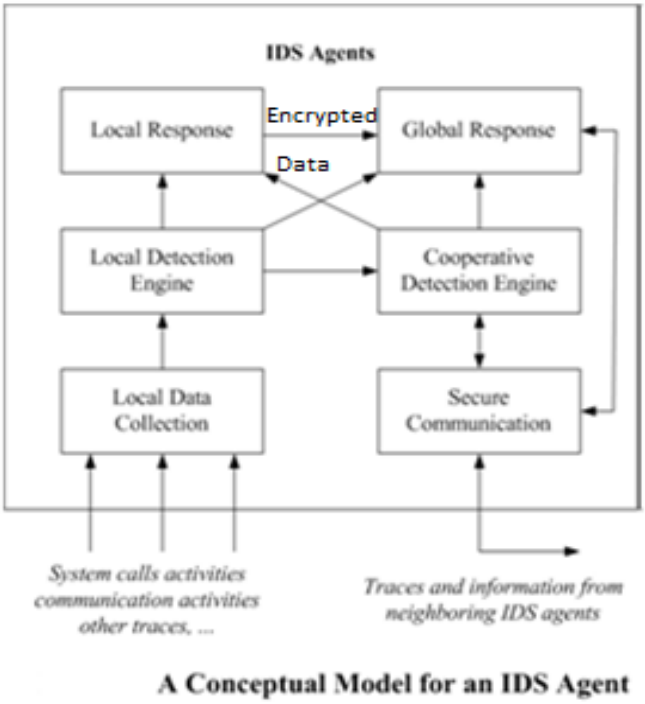

Figure 2 Conceptual Model for an IDS agent[18]

3. Cooperative detection engine, it is proficient with various IDS operators and finds more affirmations for some associating anomalies recognized to number with nodes [21][22].

4. Intrusion response module, the response to the intrusion managed after its declaration. The response could be re-booted the correspondence network, for instance, re-allotting the key, or upgrading the framework and emptying all the unsecure nodes.

4.2. Cluster-based Intrusion Detection Techniques for MANETs

A MANET could be composed out into distinctive bunches in such a way, to the point that each node is a bit of no short of what one bunch, and there will be emerge node for every gathering that will deal with the inspected issues in a certain time, is called clusterhead [23].

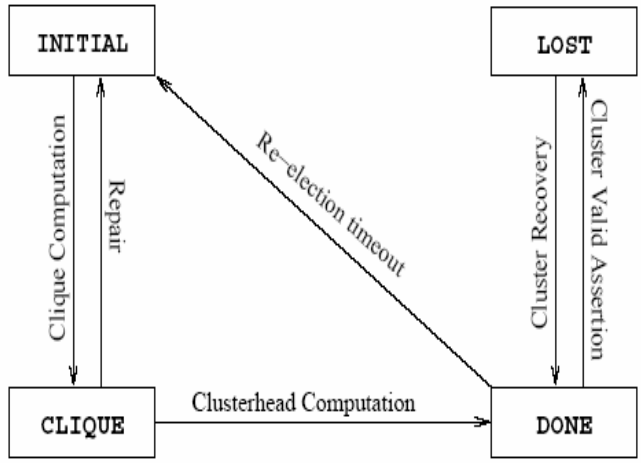

Figure 3 Cluster Formation Protocols [19]

It is essential to check the reasonability of the bunch decision technique. Here this paper suggests: the probability of every node in the pack is picked as the clusterhead should be practically identical, and every node should go about as the gathering node for the same measure of time. The finite state machine of cluster formation protocol is depicted in Figure 3.

5. CONCLUSIONS

Ad hoc networks are alterably associated network that sets up for a short time of time. Any Unfixed infrastructure in Ad hoc networks inherits the features of self-arrangement and re-development of networks. In Ad hoc networks, topology is vivacious as nodes convey the

network "on the fly" for an exceptional aim, (for example, exchanging information between one PC to another and so on). Mobile Ad hoc network (MANET) is a self forming arrangement of wireless mobile free nodes; they either unite clear or using midway node(s) with no predefined framework. According to definition the essential features of the mobile ad hoc network are acquired as: Bandwidth-synthetic, variable capacity links, Energy-synthetic operation, Restricted physical security, Self-forming, Self-healing, No Infrastructure, Peer-to-Peer, and Predominantly Wireless and Highly dynamic.

There are many important features of MANET which makes it famous, however weakness still emerges because of the inherent features of self-arrangement and re-development. Vulnerabilities are: Lack of Secure Boundaries, Dynamic Topology, and Inaccessibility of Centralized Management, Bounded Power Supply and Alterable Scalability.

Because of the routing protocols, the security of MANET is rising as extraordinary challenge. In any case, with the accommodation that the temporary UID, mobile ad hoc networks have conveyed to us, there are also security threats for the MANETs, which need to be looked into. MANET nodes are widely changing & joining the mobile network. It is unrealistic to record freed accomplished by node(s) in a dynamic network. Some of these nodes can get to be rebel and can get to be rogue as these nodes fit in with the trusted zone. This challenge is overcome by allocating a temporary id to every node.

FUTURE WORK

All through the study, I moreover discover a few focuses that could be further researched later on, for instance, a few parts of the intrusion detection techniques can get further made strides. Algorithm for allotting and releasing Temporary UID can further implemented. I will attempt to explore more in this area.

REFERENCES

[1] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, *IEEE Networks Special Issue on Network Security*, November/December 1999.

[2] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 1),* CRC Press LLC, 2003.

[3] M. Weiser, The Computer for the Twenty-First Century, *Scientific American*, September 1991.

[4] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, *IEEE Internet Computing,* pages 63–70, July-August 1999.

[5] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30),* CRC Press LLC, 2003.

[6] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02,* 2002.

[7] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9),* Springer, 2005.

[8] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31),* CRC Press LLC, 2003.

[9] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, 2003, pp. 135 – 147.

[10] Data Integrity, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Data_integrity.

[11] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January 2002.

[12] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02,* 2002.

[13] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02,* 2002.

[14] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, *Ad Hoc Networks,* 1 (1): 175–192, July 2003.

[15] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in *Proceedings of IEEE INFOCOM'03*, 2003.

[16] 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.

[17] J. R. Douceur, The Sybil Attack, in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02),* pages 251–260, March 2002, LNCS 2429.

[18] Intrusion-detection system, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Intrusion-detection_system.

[19] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in *Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000),* pages 275–283, Boston, Massachusetts, August 2000.

[20] Jim Parker, Anand Patwardhan, and Anupam Joshi, Detecting Wireless Misbehavior through Cross-layer Analysis, in *Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC'2006),* Las Vegas, Nevada, 2006.

[21] P. Krishna, N. H. Vaidya, M. Chatterjee and D. K. Pradhan, A Cluster-based Approach for Routing in Dynamic Networks, *ACM SIGCOMM Computer Communication Review*, 27(2):49–64, 1997.

[22] Sergio Marti, T. J. Giuli, Kevin Lai and Mary Baker, Mitigating routing misbehavior in mobile ad hoc networks, in *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom'00),* pages 255–265, Boston, MA, 2000.

[23] Jiejun Kong, Xiaoyan Hong, Yunjung Yi, JoonSang Park, Jun Liu and Mario Gerlay, A Secure Ad-hoc Routing Approach Using Localized Self-healing Communities, in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 254–265, Urbana–Champaign, Illinois, 2005.

BIOGRAPHIES

Miss Muskan, born on 14 July 1991, is a student at Amity Institute of Information Technology, Amity University Uttar Pradesh. Her area of interest is Computer Programming and Network Security. She is pursuing MCA from Amity Institute of Information Technology, Amity University Uttar Pradesh. She is Graduate from Maharshi Dayanand University Rohtak Haryana.

Dr. Nitin Pandey, born on 17 January 1976, is an Assistant Professor at Amity Institute of Information Technology, Amity University Uttar Pradesh. His area of interest is Coding theory, Cryptography and Network Security. He is PhD in Computer Science. M.Sc. in Mathematics from Deen Dayal Upadhaya University Gorakhpur Uttar Pradesh. He is Master of Computer Application from Maharshi Dayanand University Rohtak Haryana. He is the author and co-author of more than 14 publications in technical journals and conferences.

