IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-8 E-ISSN: 2347-2693

Security Challenges in Routing Protocols and a Proposed Schema in MANET

Mayank Kumar[1*], Muskan[2] and Rohtash[3]

[1*] *Amity Institute of Information Technology, Amity University, India, mkarya21@gmail.com*
[2] *Amity Institute of Information Technology, Amity University, India, muskanmehta14@gmail.com*
[3] *AIM College of IT & Management, G.J. University of Science & Technology, India, mittaljoy84@gmail.com*

www.ijcaonline.org

Received: 26 July 2014 Revised: 06 August 2014 Accepted: 20 August 2014 Published: 31 August 2014

***Abstract*—**A Mobile Ad hoc network (MANET) is an intelligent automated dynamically distribution of wireless Mobile independent nodes they either connect straightforwardly or utilizing halfway node(s) without any predefined infrastructure. If there is no predefined infrastructure then networks get unprotected to number of attacks and elevated amount security turns into a real concern. The first section discusses brief introduction, features and routing protocols of MANET. The second section discusses the vulnerabilities in MANET. Mobile ad-hoc network (MANET) is one of the most necessary fields for study, development and research of wireless networks. Mobile Ad Hoc Networks (MANETs) has become one of the most frequent areas of research because of the security challenges it faces to its related protocols. The third section discusses the security challenges in routing protocols in MANET. The final section discusses Intrusion Detection Techniques (IDT), IDS architecture and conceptual model of IDS agent. MANET nodes are extensively changing & joining the mobile network. It is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can become rogue and can become danger as these nodes belong to the trusted zone. This challenge is overcome by assigning a temporary id to each node. The paper proposes a novel algorithm to generate and assign a unique id for the nodes that are freed.

***Keywords*—** Mobile Ad Hoc Networks, attacks, IDS, Routing Protocols, Schema, Temporary UID Algorithm

I. INTRODUCTION

Network technology has become very substantial aspect and has many influences on people's life such as exchanging resources, information and data smoother and faster. Wi-Fi, APN, Wi-MAX are the various networks which helps people to share resources, transfer related information and important data between different types of devices all across the world [1].However, the same network technology and techniques have been used by people to hack and attack the network with growing data flow inbound and outbound in.

Mobile Ad hoc network (MANET) is a self-forming arrangement of wireless mobile independent nodes; they either connect straightforward or utilizing halfway node(s) without any predefined infrastructure. The unfixed infrastructures and routers have capability to move independent anywhere without any restrictions. Mobile has antennas that receives and transmits information. Hence, self organizing networks combines' mobile wireless communications with high degree node flexibility, independence and mobility [2] [3]. The users make use of many electronic platforms though which they can access all the relative data and information whenever and wherever they are [2]. Also, MANET nodes can communicate directly with other nodes within the transportation ranges, whereas nodes those are not in their transportation range use intermediate node(s) to communicate therefore this composition of wireless networks can be represented as MANET.

Features of MANET are inherited as [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.

Corresponding Author: *Mayank Kumar, mkarya21@gmail.com*

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 discusses the number of vulnerabilities that are inherited from the given features of MANET. Organization of paper has been done as follows. The second section discusses the vulnerabilities in MANET in details. Due to the features of routing protocols, the security of MANET is emerging as great challenge. The third section discusses the security challenges in routing protocols in Mobile Ad hoc network. The final section discusses Intrusion Detection Techniques (IDT), IDS architecture and conceptual model of IDS agent. MANET nodes are extensively changing & joining the mobile network. It is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can become rogue and can become danger as these nodes belong to the trusted zone. This challenge is overcome by assigning a temporary id to each node. The paper proposes a novel algorithm to generate and assign a unique id for the nodes that are freed.

II. VULNERABILITIES OF MANETs

There are many important features of MANET which makes it popular, but vulnerability still arises due to the inherent features of self-configuration and re-formation. A detailed discussion for the reasons is mentioned below:

1. Lack of Secure Boundaries

Nodes inside MANET have no restriction for nodes to connect, join, disconnect and travel in or out side of the network. Thus, the lack of safety measures makes the MANET prone to the attacks. The MANET is open to attack due to lack of firewall and network gateway [6].

2. Dynamic Topology

Since, nodes are changing & joining the mobile network. It is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can become rogue and can become danger as these nodes belong to the trusted zone [10].

3. Inaccessibility of Centralized Management

There is no operation control centre i.e. unified administration office, for MANET i.e. a name server, which prompts some defenseless challenges. Hence it becomes difficult to screen the activity in a profoundly dynamic and expansive scale network [7]. This issue results in breakdown and failure in transmitted information. Hence, nodes do not contribute in any security operations. A deficiency of this type cause can hamper the overall operations of the nodes connection and disjoints [5][8][11].

4. Bounded Power Supply

The nodes depend completely on the battery as their energy supply technique. This is a limited type of power supply. The failure discussed can exist in a spite second causing numerous challenges compared to the wired network [13].

5. Alterable Scalability

All in all wired network scale is predefined when outlined and not change such throughout the utilization, however scale is changing every time in light of versatility in MANET. There is no network to predict number of nodes in MANET. This implies that network needs scale up and down at each one time in network [14].

III. SECURITY CHALLENGES IN ROUTING PROTOCOLS IN MANET

3.1 Attacks on Routing Protocols

Ad-hoc networks are more easily challenged rather than other wired network. The challenges predominant on ad-hoc routing protocols are characterized as- Passive Attack are not able to disturb the behavior of the protocol, yet reveal gainful information by tuning into movement. Passive attacks in a general sense incorporate gaining essential routing information by sniffing about the network. Such attacks are ordinarily troublesome to place and in this manner, guarding

against such attacks is bewildered. Notwithstanding the way that it is not possible to recognize the exact region of a node, one may have the ability to reveal information about the network topology, using these attacks. An Active Attack, however, imbues subjective bundles and tries to exasperate the operation of the protocol remembering the finished objective to cutoff openness, get confirmation, or force in parcels bound to distinctive nodes. The target is in a far-reaching way to attract all bundles to the attacker for examination or to weaken the network. Such attacks could be placed and the nodes may be recognized [15].

3.2 Attacks on MANETs

There are different types of attacks in on MANETs, but most recognize attacks are [12]:

3.2.1 Eavesdropping Attacks

Eavesdropping is known as exposure attacks, typically done by outer or inner nodes and is passive. The attacker's objective of Eavesdropping is to break down broadcast messages and acquire some helpful data about the network that is mystery throughout the correspondence [9].

3.2.2 Denial of Service (DoS)

In DoS attacks, attackers attempt to attack at the accessibility of administrations of the whole Mobile Ad hoc network. The attackers utilize the battery depletion methods and the radio sticking 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 deliberately drops all the packets that are not bound for them. In dropping attack, vindictive nodes intend to disturb the association, while egotistical nodes plan to safeguard their assets. It decreases the network execution by bringing on information bundles to be transmitted once more; new routes to the destination are to be found.

IV. PROPOSED SECURITY SCHEMA IN MANETs

Intrusion Detection Techniques (IDT)

There are a number of difference between the wired network and the MANET, Intrusion detection system is first established in the wired network and has transformed into the necessary principal security respond in due order regarding the wired network, has additionally gotten a couple of contemplations from the investigators when they research the security respond in due order regarding the MANET. In the accompanying, some ordinary interruption recognition methods in the mobile ad hoc networks in points of interest [16][17].

4.1. Intrusion Detection Techniques (IDT) in MANET

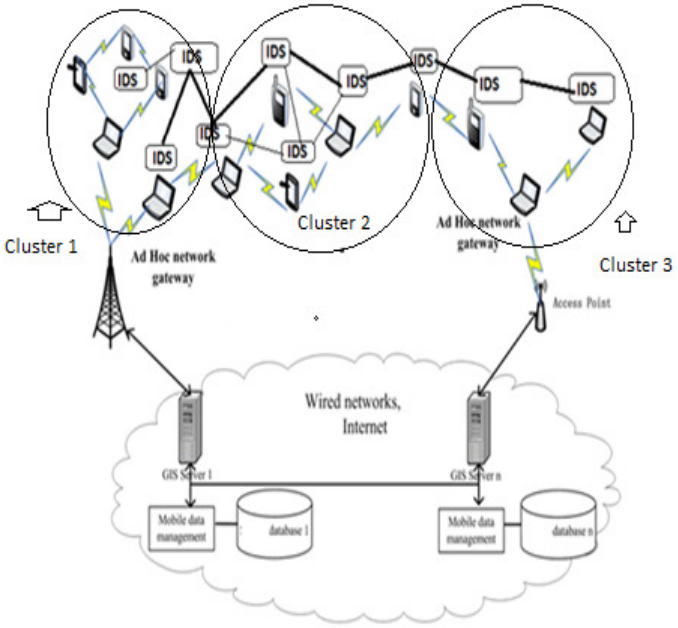

Figure 1 Intrusion Detection System for MANET [20]

In this architecture (figure 1), each node in the MANETs takes an interest in the IDT process and response practices by distinguishing tracks of intrusion conduct by regional standards and uninhibitedly, which are established by the inherent Intrusion Detection System agent. However, the nodes may offer their controlled results to everyone thus and join in a wide physical field. The collaboration in nodes customarily occurs when a node gets usually yet not having enough confirmation to finish what sort of intrusion it interfaced to.

In the conceptual model, Main functional modules are:

1. Local data collection module, basically manages the data get-collection problem, the ongoing review data may originate from different radio resources.
2. Local detection engine examines at the local data gathered by the local data collection module and investigates to check the inconsistency indicated in the information.
3. Cooperative detection engine, it is accomplished with a number of IDS agents and discovers more confirmations for some suspecting anomalies distinguished to number of nodes [21][22].
4. Intrusion response module, the reaction to the intrusion managed after its declaration. The reaction could be re-booted the correspondence network, for example, re-assigning the key, or redesigning the system and evacuating all the unsecure nodes.

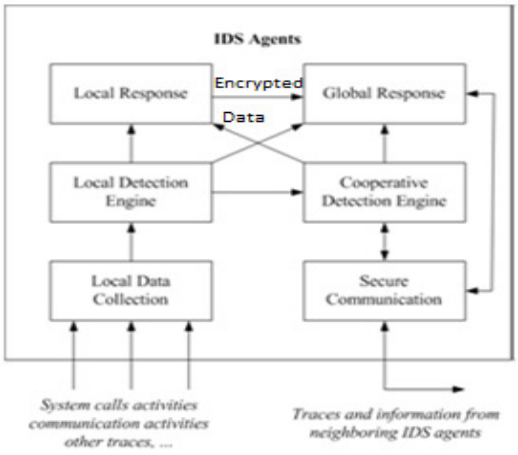

Figure 2 Conceptual Model for an IDS agent[18]

4.2. Cluster-based Intrusion Detection Techniques for MANETs

A MANET could be written out into different bunches in such a way, to the point that every node is a piece of no short of what one bunch, and there will be emerge node for each group that will manage the examined problems in a certain time, is called clusterhead [23].

It is important to check the viability of the bunch decision technique. Here this paper suggests: the likelihood of each node in the bunch is picked as the clusterhead ought to be comparable, and each node ought to go about as the group node for the same measure of time. The finite state machine of cluster formation protocol is depicted in Figure 3.

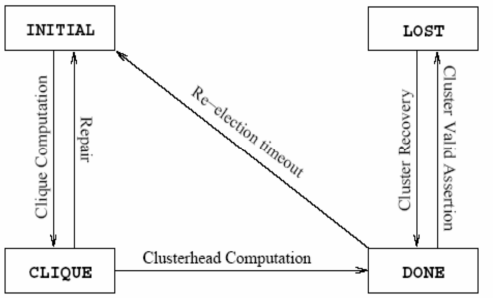

Figure 3 Cluster Formation Protocols [19]

4.2.3 Temporary UID Assigning to Each Node

MANET nodes are extensively changing & joining the mobile network. It is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can become rogue and can become danger as these nodes belong to the trusted zone. This challenge is overcome by assigning a temporary id to each node. The paper proposes a novel algorithm to generate and assign a unique id for the nodes that are freed. Temporary unique identification is to be assigned to each node that belongs to the cluster from a pool of IDs. As the nodes become free, the UID will be released and its information will be stored in the pool of the database. This will help the MANET to protect the vulnerabilities issues arising due to rogue freed nodes and MANET becomes more accountable.

Algorithm for assigning and releasing Temporary UID

Step 1: Given,

Number of clusters says C_i

Number of nodes in a cluster, says N_i

Ni is a node.

U_{id} be the Temporary Unique ID.

T_j be the time to live for the node in cluster.

Step 2: Set C_i

Step 3: Repeat Step 3 through 5 for all i = 1…….N

Step 4: Set N_i

Step 5: Repeat Step 5 through 7 for all i = 1…….N

Step 6: Generated and Assign U_{id} to N_i from the IDs pool of database

Step 7: Set T_j to N_i

Step 8: Repeat Step 8 through 11 for all j = 1…….N

Step 9: If T_j becomes zero

Step 10: Identify the N_i for all i = 1…….N

Step 11: Free the N_i

Step 12: Repeat Step 12 through 14 for all i = 1…….N

Step 13: Release the U_{id}

Step 14: Store the information of U_{id} in the IDs pool of database

V. CONCLUSION

Ad hoc networks are dynamically connected network that sets up for a short period of time. Any Unfixed infrastructure in Ad hoc networks inherits the features of self-configuration and re-formation of networks. In Ad hoc networks, topology is vigorous as nodes communicate the network “on the fly” for a special intention (such as transferring data between one computer to another etc). Mobile Ad hoc network (MANET) is a self forming arrangement of wireless mobile independent nodes; they either connect straightforward or utilizing halfway node(s) without any predefined infrastructure. As per definition the essential features of the mobile ad hoc network

are inherited 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 popular, but vulnerability still arises due to the inherent features of self-configuration and re-formation. Vulnerabilities are: Lack of Secure Boundaries, Dynamic Topology, and Inaccessibility of Centralized Management, Bounded Power Supply and Alterable Scalability.

Due to the features of routing protocols, the security of MANET is emerging as great challenge. However, with the accommodation that the temporary UID, mobile ad hoc networks have brought to us, there are additionally security dangers for the MANETs, which need to be taken into consideration. MANET nodes are extensively changing & joining the mobile network. It is not possible to record the freed accomplished by node(s) in a dynamic network. Some of these nodes can become rogue and can become danger as these nodes belong to the trusted zone. This challenge is overcome by assigning a temporary id to each node. The paper proposes a novel algorithm to generate and assign a unique id for the nodes that are freed. Temporary unique identification is to be assigned to each node that belongs to the cluster from a pool of IDs. As the nodes become free, the UID will be released and its information will be stored in the pool of the database. This will help the MANET to protect the vulnerabilities issues arising due to rogue freed nodes and MANET becomes more accountable.

Future Work

Throughout the study, we additionally discover a few focuses that could be further investigated later on, for example, a few parts of the intrusion detection techniques can get further made strides. Algorithm for assigning and releasing Temporary UID can further implemented. We will attempt to investigate deeper in this area.

Reference

[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] Mayank Kumar and Tanya Singh, A survey on Security Issue in Mobile Ad-hoc Network & Solutions, International Journal of Computer Science and Engineering, pages 68-72, March 2014.

[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.

