Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review Paper on the Study of MANET, Various Attacks with Its Detection Schemes, Various Trust-based Models for Reliable and Secure Reactive Routing

Meera N. Hapaliya, Naren V. Tada [Assistant Professor]
Department of Computer Engineering,
V.V.P. Engineering College,
Gujarat, India

Abstract - A Mobile Ad Hoc Network (MANET) is a set of self-configurable mobile nodes which communicate with each other over wireless links and does not rely on fixed-infrastructure for its operations. Mobile Ad Hoc Network is having features of self-creation, self-organization & self-administration.Because of the fundamental characteristics like wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks. Thus to mitigate various security challenges during routing ,there are various detection and prevention techniques categorized & also routing protocols according to criteria such as routing information update mechanism, based on the use of temporal information for routing ,routing topology based and based on the utilization of specific resources.In this paper we study mobile ad-hoc network and its characteristics, challenges, applications, security goals, different types of security attacks at different layers, various detection techniques and trust-based routing protocols for secure and reliable reactive routing in MANETs.

Keywords - Mobile Ad-hoc Network(MANET), Ad-hoc On-demand Distance Vector routing (AODV), Flooding attack, Blackhole attack, Intrusion Detection Scheme (IDS)

I. INTRODUCTION

A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations.[4] As MANET has no fixed infrastructure, they are more prone towards the security threats as compared to the infrastructure wireless networks.

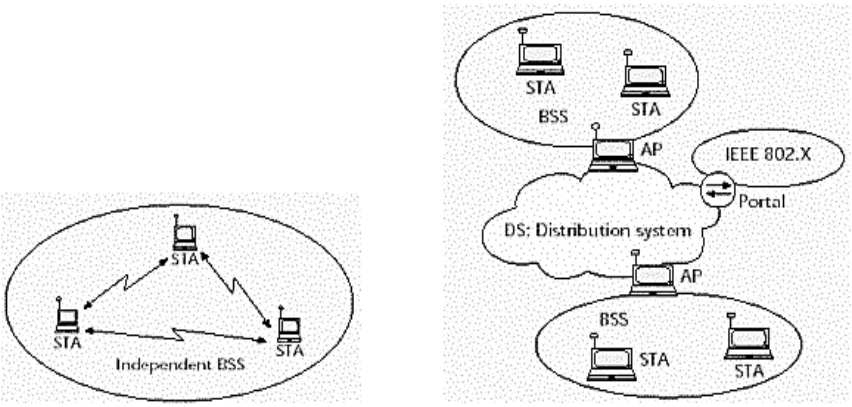

Fig. 1 Ad-hoc vs. Infrastructure mode of Routing\

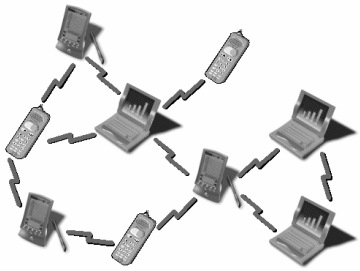

Fig. 2 Example of Mobile Ad-hoc Network

© 2015, IJARCSSE All Rights Reserved

A.MANETS CHARACTERISTICS

The characteristics of MANET are as below[4]:-

(1) *Distributed Operation:* There is no background network for the central control of the network operations; the control of the network is distributed among the nodes.
(2) *Multi hop routing:* When a node tries to send information to other nodes which is out of its communication range, at that time the packet should be forwarded via one or more intermediate nodes.
(3) *Autonomous terminal:*In MANET, each mobile node is an independent node, which could function as both a host and a router.
(4) *Dynamic Topology:*The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.
(5) *Light-weight terminals:*In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.
(6) *Shared Physical Medium:*The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

TABLE I APPLICATIONS OF MANET

Application	*Possible Scenarios/Services*
Tactical networks	– Military communication & services – Automated battlefields
Emergency services	– In disaster recovery – For search and rescue operations – Supports doctors and nurses in hospitals
Educational	– In virtual classrooms – Ad-hoc communications during meetings and lectures – For universities and campus settings
Entertainment	– Multi-user games and robotics – Theme parks – Outdoor Internet access service
Wireless sensor networks	– For body area network – In data-tracking such as animal movements, chemical detection, whether conditions
Commercial sectors	– For e-commerce and business transactions – In vehicular services – In sports stadiums – In shopping malls

B. ADVANTAGES OF MANETS

Below are the advantages of MANETs[4]:-

(1) Provides an access to information and services regardless of geographic position.
(2) Independence from central network administration. So, nodes are also act as routers.
(3) Less expensive as compared to wired network.
(4) Scalable that means accommodates the addition of more nodes.
(5) Improved Flexibility.
(6) Also Robust due to decentralize administration.
(7) The network can be set up at any place and time.

C.SECURITY CHALLENGES OF MANETS

Various security challenges are as below[4]:-

(1) Wireless link continue to have significantly lower capacity than infrastructure networks, due to *Limited Bandwidth*.
(2) Due to *Dynamic topology* membership may disturb the trust relationship among nodes.
(3) In wireless ad hoc networks, nodes often change their location within network which leads to some stale routes and *Routing Overhead*.
(4) The *Hidden terminal problem* refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
(5) Due to these *transmission errors* like the presence of hidden terminals, presence of interference, unidirectional links, and frequent path breaks due to mobility of nodes, *Packet loss* is being occurred.
(6) *Frequent route changes*situation can be occurred due to highly dynamic network topology and movements of nodes.

© 2015, IJARCSSE All Rights Reserved

(7) Devices used in these networks have restrictions on the *power source* in order to maintain portability, size and weight of the device.

(8) Some *Security threats* are also there, that means Threat is the way through which the ability or intent of an agent to adversely affect an automated system, facility or operation can be manifested[8].

D. Security Goals of MANETs

Considerable security goals are as below[4]:-

(1) *Availability:* Availability means the assets are accessible to authorized parties at appropriate times.

(2) *Confidentiality:* Confidentiality ensures that computer-related assets are accessed only by authorized parties.

(3) *Integrity:* Integrity means that assets can be modified only by authorized parties or only in authorized way.

(4) *Authentication:*It is essentially assurance that participants in communication are authenticated and not impersonators.

(5) *Authorization:* This property assigns different access rights to different types of users.

(6) *Resilience to attacks:* It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

(7) *Freshness:* It ensures that malicious node does not resend previously captured packets.

E. Vulnerabilities of MANETs

It is a weakness in security system. MANET is more vulnerable than wired network. Thus, some of the vulnerabilities are as following[4]:-

(1) *Lack of centralized management:* MANET doesn't have a centralized monitor server.

(2) *No predefined Boundary:* In mobile ad-hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network.

(3) *Cooperativeness:* In MANETs , the nodes are cooperative and non-malicious

(4) *Limited power supply:* The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems like malicious behaviour.

(5) *Adversary inside the Network:* The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously.

II. TYPES OF ATTACKS AND ROUTING PROTOCOLS

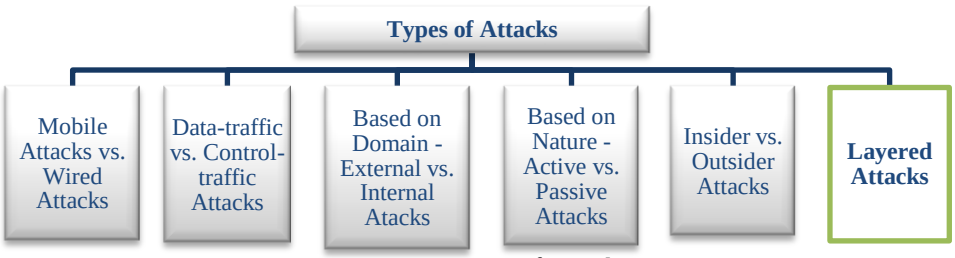

Fig. 3Various Types of Attacks

TABLE II LAYERED ATTACKS

Layer	*Problems*	*Attacks[2]*
Application	– LDA – Service discovery security	– Repudiation – Attack by virus & worms
Transport	– TCP, – QoS	– TCP SYN attack (DOS attack) – TCP Session Hijacking – Jelly Fish attack
Network	– **Routing,** – **Addressing,** – **Location management**	– **Flooding attack (DOS attack)** – **Route tracking** – **Message Fabrication and modification** – **Black hole attack [27]** – **Wormhole attack [27]** – **Grayhole attack** – **Rushing attack** – **Link spoofing attack** – **Byzantine attack** – **Sybil attack**
MAC (Data-Link) Layer	– Bandwidth, – Congestion and Traffic	– Traffic monitoring & Analysis – Bandwidth Stealth

© 2015, IJARCSSE All Rights Reserved

		– MAC targeted attack
		– WEP targeted attacks
Physical	– Channel access, – Power control, – Multiuser detection	– Jamming attack (DOS attack)
		– Stolen or compromised attack
		– Malicious message injecting
		– Eavesdropping attack

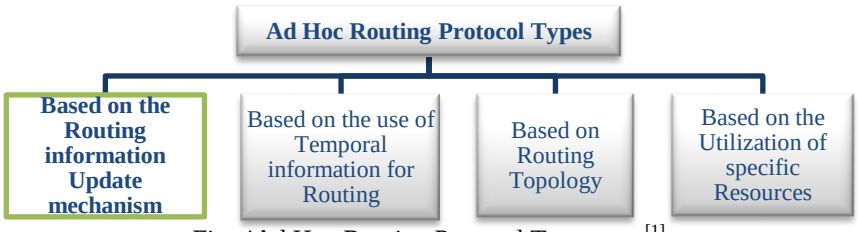

Fig. 4Ad Hoc Routing Protocol Taxonomy[1]

TABLE III MOBILE AD-HOC ROUTING PROTOCOL CLASSIFICATION

Based on the routing information update mechanism MANET routing protocols[1] [7]	
Proactive or table-driven routing protocols (DSDV, WRP, STAR, CGSR)	Proactive or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.
Reactive or on-demand routing protocols **(DSR, AODV)**	**Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network.**
Hybrid routing protocols (ZRF, TORA, OORP, ARPAM)	They introduce a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory.

III. TRUST BASED ROUTING PROTOCOLS

TABLE IV COMPARISON OF VARIOUS TRUST BASED ROUTING PROTOCOLS [5][6]

Protocol	*Advantage*	*Disadvantage*
TAODV	– TAODV can detect malicious node and selfish node in network – It is more secure and having better performance than AODV – It can prevent modification, fabrication attacks	– It has no authentication mechanism of nodes and messages – It can't prevent worm-hole and impersonation attack
Cooperation Of Nodes: Fairness In Dynamic Ad-Hoc Networks(CONFIDENT)	– CONFIDANT protocol effectively detect selfish nodes and PM wormhole nodes that drop packets	– It can't prevent various attacks such as modification, impersonation, fabrication, Sybil attack by malicious nodes – An attacker is able to send false alarm messages and can do false claim that a node is misbehaving
Friendship Based AdHoc On Demand Distance Vector(FrAODV)	– This protocol gives better performance in terms of QoS services like packet delivery fraction, normalized routing load.	– The end to end delay is not included in performance measurement metric. – The delay is more here because two evaluation algorithms are used to establish path.

© 2015, IJARCSSE All Rights Reserved

Secure Routing using Trust (SRT)	– In terms of mobile mobility it gives better throughput, packet delivery ratio, average path length, average routing load.	– The performance decreases in the presence of attacks except black hole. – The trust is calculated on the basis of control packets only.
Trusted AOMDV	– Performance is measured in terms of route selection time, trust compromise TDSR,AOMDV etc.	– This protocol measures the performance in fixed mobility.
Friend Based Ad HocRouting Using Challenges To Establish Security(FACES)	– Challenge packet helps to detect flooding, grey-hole, spoofing, modification, dropping of control packets. – Also it gives better performance in the presence of malicious nodes.	– In this protocol control overhead is increased due to periodic flooding of challenge packet and periodic sharing of friend list.
Trust Based SecurityProtocol(TBSP)	– This protocol maintains confidentiality and authenticates the nodes based on digital signature. – It detects the nodes which are misbehaving.	– This protocol can't detect authenticated malicious node. In this protocol after finding route then the trust of the nodes along the path is calculated which increases control overhead. – Because calculating the trust after finding path is inefficient as the path may be rejected due to presence of malicious nodes.
Trust based DSR	– It gives better throughput with general DSR.	– This protocol measures the performance in fixed mobility environment that actually not applicable in MANET.
NDTAODV	– Provides security against RREQ flooding attacks in existing AODV routing protocol to establish a secure route for communication	– Packet Delivery Fraction (PDF) of NDTAODV improve and Average Throughput (AT) which is the most important aspect of protocol is maintained as the pause time increase while AODV performance drops significantly under the presence of flood attack.

IV. VARIOUS INTRUSION DETECTION SCHEMES

The mobile nodes are independent and there movement is not controlled by the system. So the nodes can easily be captured & compromised. The architecture of wireless network also has no physical obstacles, so attacks can come from any directions.Adversaries can exploit the decentralized management, by breaking the cooperative algorithm. To tackle this situation different IDS are available, such like[3]:-

(1) *Standalone IDS:* Every node has its own IDS agent, which monitor the node only, if any threat has been detected then it can take protection locally & since there is no cooperation between nodes then all decisions are based on information collected by nodes. This method is not so proficient.

(2) *Cooperative IDS:* Wireless ad hoc network is distributed in nature so the detection & response mechanism must be in two phase. Local & Global detection. Every node has IDS agent that detect attacks locally and cooperates with other nodes inside network and inform globally. Significantly, this distributed-cooperative IDS technology mush more stable than standalone IDS and more stable form flat, cluster based network configuration.

(3) *Hierarchical IDS:* Here also every node has its own IDS agent. Collection of nodes form cluster. Every cluster has a special node know as cluster head.IDS agent for cluster head in responsible for both local & global Intrusion detection. Layered architecture in wireless ad hoc network can be protected by this approach. Another alternative distributed solution called spontaneous watchdog. Fast sensor ad hoc network without divide them into clusters, some powerful independent, spontaneous nodes are created, known as watchdog, which monitors the communication with their neighbors.

(4) *Zone based IDS:* The local IDS agent used in Zone based Intrusion detection system (ZBIDS).Zone can be formed by geographic partitions. Every node has its two identities, INTRA ZONE and INTERZONE & can be determined by Zone ID. By forwarding HELLO Message, inter and intra zone nodes are determined. A node may change its role by the nature of mobility.

© 2015, IJARCSSE All Rights Reserved

V. CONCLUSION

After studying MANET and reviewing various trust based routing protocols and trust based models, we have conclude that our proposed trust model for secure and reliable routing will consider trust computation (direct trust), node's trust calculation and path's trust calculation. And its basic routing flow includes main stages like route discovery, route selection, trust updation and malicious node detection in AODV routing protocol. During Simulation, we will measure various network performance parameters like Packet delivery ratio, Average end-to-end delay, Routing overhead and Path optimality in NS-2. In future, we want to make our trust model in AODV routing protocol in such a way that it can prevent and detect more number of possible network layered attacks in MANETs.

REFERENCES

[1] K. Vanitha, Dr. A. M. J. Md. Zubair Rahman, K. Anitha ,"An Analysis of Issues in Security and Routing Protocol in MANET", *in Proceedings of* International Journal of Engineering Research & Technology (IJERT) , ISSN: 2278-0181 , Vol. 3, Issue 1, January – 2014

[2] Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamali, "Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network", *in Proceedings of* International Journal of Computer Applications Technology and Research (IJCAT), Volume 3– Issue 9, 541 - 546, 2014

[3] Maulik H. Davda, Sheikh R. Javid, "A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes", *in Proceedings of* International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS), ISSN: 2321-7782 (Online), Volume 2, Issue 4, April 2014

[4] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Software Engineering (IJARCSSE), ISSN: 2277-128X, Volume 3, Issue 5, May 2013

[5] Mousumi Sardar, Koushik Majumder, "A SURVEY ON TRUST BASED SECURE ROUTING IN MANET", *in Proceedings of* David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA – 2013,pp. 243–253, 2013.

[6] Dr. Akshai Agraval,Savita Gandhi, Nirbhay Chaubey, Naren Tada, Srushti Trivedi, "NDTAODV: Neighbor Defense Technique for Ad hoc On-Demand Distance Vector (AODV) to Mitigate Flood Attack in MANETs", *in Proceedings of*International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014

[7] Savita Gandhi, Nirbhay Chaubey, Naren Tada, Srushti Trivedi, "Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANETs", *in Proceedings ofComputer Communication and Informatics (ICCCI), 2012 International Conference of*IEEE, Coimbatore, 10-12 Jan. 2012

[8] Farooq Anjum, Petros Mouchtaris, "Security for Wireless Ad Hoc Networks", *in Proceedings of* WILEY-INTERSCIENCE A JOHN WILEY & SONS, INC., PUBLICATION, 2007

AUTHORS PROFILE

[1] **Meera N. Hapaliya,**Received the B.E. degree in Computer Engineering from R.K. University and Pursing M.E. degree in Computer Engineering from V.V.P. Engineering College. Her areas of interests are Networking, Security Mechanism.

[2] **Naren V. Tada,** Assistant Professor at the Department of Computer Engineering in V.V.P. Engineering College. He did his M.Tech from Gujarat Technological University and has published many Papers in International journals and guiding M.E./M.Tech Scholars in the fields of Computer Engg.

© 2015, IJARCSSE All Rights Reserved