Detection and Prevention Scheme against Jamming Attack in MANET

Namrata Soni
M.Tech Scholar in Dept. of CSE
SISTec, Gandhi Nagar, Bhopal, India

Vinay Singh
Dept. of CSE
SISTec, Gandhi Nagar, Bhopal, India

ABSTRACT

In Mobile Ad hoc Network nodes are established connection and deliver data in dynamic environment. Security is the one amongst the most important problem in Mobile ad hoc Network (MANET). Owing to distinctive characteristics of MANET, it creates variety of important challenges to its security design to beat the challenges, there's a desire to create a security scheme that achieves both in depth protection and fascinating network performance from attacks. In mobile ad hoc networks wherever the constellation animatedly changes, straight ways can't be used with efficiency. The various security schemes against attack are improves the network performance in presence of offender to disable misbehaviour activity. In this paper we tend to examine the behaviour of various attacks result in network. In this survey we majorly highlight the behavior of different attacks with specific consistence of Jamming attack and defense schemes in MANET. The multipath routing schemes is also discussed to improve the network performance in network but condition is that jamming condition are possible to occur by attacker. In presence of attacker security scheme are always provides the secure path then in multipath routing the possibility of secure routing is enhanced in presence of attacker and security scheme.

Keywords
Security, Attack, Routing, MANET, Multipath

1. INTRODUCTION

Mobile ad-hoc network could be a self organizing network that consists of mobile nodes that are capable of communication with one another while not the assistance of fastened infrastructure. On the contrary to ancient wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals [1]. Two nodes will have multiple links between them for communication and deployed in an exceedingly complete fashion, appropriate for price and time effective setting, and for a scenario wherever infrastructure is troublesome to setup. Security is difficult in MANETs [2] attributable to its characteristics like peer to see design, operational while not central arranger, dynamic topology, insecure operational setting, and frequent link breakage attributable to mobile nodes, battery period of time, machine capability and non uniformity [3]. Communication in MANETs is thru single hop in link layer protocols and multi hop in network layer protocols, supported the belief that each one the nodes in an exceedingly network are cooperative in coordination method, however sadly this statement isn't true in hostile setting. Malicious attacks [2] will simply disrupt network operation by violating protocol specifications. The network layer operations in MANET are supported routing and knowledge packet forwarding each are susceptible to malicious attacks.

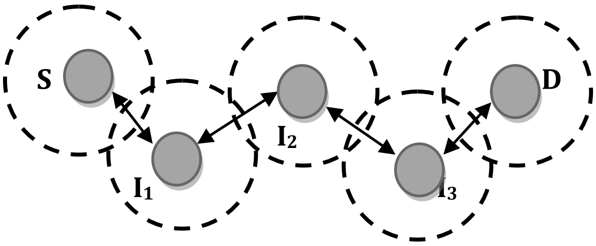

Fig 1: Ad Hoc Network

Mobile ad-hoc networks lack permanent infrastructure and use wireless link for interaction makes them terribly susceptible to an adversary's Mobile ad-hoc networks are inclined to an outsized range of security threats, the essential reality that malicious attacks.

Attackers are severe security threats in ad-hoc networks which may use with no trouble by exploiting susceptibleness of on-demand routing protocols like AODV. This tries to use Intrusion Detection (ID) to stop attacks obligatory by each single and multiple nodes and therefore the Detection and healing routing misbehaviour below MANET. we try to reach up to the specific solution maximizes network performance by the help of minimizing production of control (routing) packets as well as successfully opposing attacks against mobile ad-hoc networks [1].

2. MANET SUSCEPTIBILITIES

Susceptibility is a weakness in security system. A meticulous system may be susceptible to illegal data manipulation because the system does not verify a user’s distinctiveness before allowing data access [2, 6]. MANET is more susceptible than wired network. Some of the susceptibilities are as follows:

2.1 Absence of Centralized Authority

MANET doesn’t have a centralized authority. The absence of centralized authority makes the detection of attacks difficult because it is not east to monitor the traffic in a vibrant and large scale MANET.

2.2 Lack of Predefined Boundary

In MANET we cannot exactly identify a substantial boundary of the network. The nodes work in a itinerant environment where all nodes are free to join and leave the network at any instance of time. As soon as an opponent comes in the radio range of a node it will be able to communicate with that node.

2.3 Supportive in Communication

The Routing protocol of MANETs usually assumes that mobile nodes are cooperative and reliable (not malicious). The routing misbehavior through malicious attacker can easily become disrupts network operation.

2.4 Limited power supply

The nodes in MANET are completely performing energy or power dependent operations need to consider restricted power supply, which will cause several problems. A node in MANET may behave in a selfish manner when it is finding that there is only limited power supply.

2.5 Opponent inside the Network

At any time instant, the assumed nodes within network may additionally conduct maliciously. In dynamic network it is severe to distinguish that the behavior of the node is malicious attacker. Attack is harmful on that kind of network.

3. ROUTING PROTOCOLS IN MANET

In dynamic network the topology is regularly changes that are the cause of link breakage are created as multiple-hop till the destination is not found. The routing protocol is playing a essential part at network layer for data accepting and forwarding through every router or node the data is cause by sender and accepted by receiver in that procedure routing strategy is very important part of communication [4, 5]. For connecting to end and information delivery the routing protocol is necessary for routing the data in between sender to receiver every routing protocol has different routing approaches of link establishment however has same method of select shortest path in between sender and receiver. The direct path is decided on the basis of least hop count importance in manet. The classifications of routing protocols in manet are as follows:-

3.1 Proactive Routing Protocol

The proactive routing protocols are also called as are maintaining the routing information of each node counter driven routing protocol and these routing protocols that are collaborate in routing procedure. In Mobile ad hoc network the topology in network is change by that the transparency of maintain the information of each node is extremely complex and required immense arrangement of memory for store routing information in network. In ad hoc network if the nodes are moves at slow speed then that protocol is assume to be better for communication. The example of proactive routing protocol is DSDV routing protocol.

3.2 Reactive Routing Protocol

The Reactive routing protocols are also called as on demand routing protocol and these routing protocols are maintain the routing information on the basis of demand of request receives by the neighbor. There is no routing information is stored of each node that are collaborate in routing procedure. In Mobile ad hoc network the topology in network is change by that the overhead of maintain the information of each node is not desired to maintain. In ad hoc network if the nodes are move at random speed then that protocol is supposes to be enhanced for communication. The example of reactive routing protocol is AODV routing protocol.

3.3 Hybrid Routing Protocol

Proactive and reactive protocols every work preeminent in oppositely different scenario, hybrid method uses both. it is used to find a balance between both protocols. Proactive operations square measure restricted to small domain, whereas, reactive protocols square measure used for locating nodes outside those domains.

4. SECURITY THREATS IN MANET

The current mobile ad-hoc networks provide many various kinds of attacks. Although the analogous exploits put together exits in wired networks but it's easy to repair by infrastructure in such a network. Current MANET square measure primarily at risk of two differing types of attacks: active Attacks and passive attacks. Active attack is attack once misbehaving node should accept those energy costs so on perform the threat [6]. On the other hand, passive attacks square measure within the main attributable to lack of cooperation with the aim of saving energy selfishly. Nodes that perform active attacks with the aim of damaging totally completely different nodes by inflicting network outage square measure thought-about as malicious whereas nodes that make passive attacks with the plan of saving battery life for his or own her communications square calculate thought-about to be mean[7].

5. TYPES OF ATTACK IN MANET

There are various kinds of attacks within the mobile ad hoc network, nearly all of which can be classified as the following two types.

5.1 External attacks

In External attack, attacker aims to cause congestion, propagate replica routing information or disturb nodes from providing services.

5.2 Internal attacks

In Internal attack the adversary wants to gain the normal access to the network and involve you within the network behavior, either by some malicious impersonation to find the access to the network as a new node, or by directly compromise a existing node and using it as a basis to conduct its malicious behaviors. in the two categories shown above, external attacks square measure similar to the normal attacks within the traditional wired networks in that the adversary is within the proximity but not a reliable node within the network, therefore, this kind of attack can be prohibited and detected by the security methods such as membership authentication or firewall, that square measure relatively typical security solutions.

However, due to the pervasive communication nature and open network media within the mobile ad hoc network, internal attacks square measure far extra dangerous than the internal attacks: because the compromised nodes square measure originally the benign users of the ad hoc network, they can simply exceed the authentication and get protection from the security mechanisms.

As a result, the adversaries can make use of them to gain normal access to the services to facilitate should only be available to the authorized users within the network, and they can use provided by the compromised nodes to hide their malicious behaviors. Therefore, we must always pay extra attention to the internal attacks initiated by the malicious insiders once we consider the safety problems in the mobile ad hoc networks.

In the following, we discuss the most attack sorts that emerge in the mobile ad hoc networks.

5.3 Flooding Attack

Flooding attack [9] may be a denial of service method of attack at intervals which the malicious node broadcast the unnecessary false packet in the network to consume the on the market resources so that valid or legitimated user can't able to use the network resources for valid communication. Because of the restricted resource constraints in the mobile ad hoc networks resource consumptions a result of flooding attack reduces the throughput of the network.

The flooding attack is probable in all most all the on require routing, relying upon the type of packet used to flood the network, flooding attack can be classified in two classes.

5.4 RREQ FLOODING

RREQ flooding data flooding RREQ flooding in the RREQ flooding attack, the attacker broadcast the various RREQ packets per time interval to the IP address that doesn't exist in the network and disable the restricted flooding feature. On demand routing protocols uses the route discovery process to support the route connecting the two nodes. In the route detection the availability node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher than information packet then at the high load also RREQ packet are transmitted. A malevolent node exploits this feature of on demand routing to launch the RREQ flooding attack.

5.5 Jamming Attack or Data Flooding

In the data flooding, malicious node flood the network by sending useless data packets. To start the data flooding, first malicious node engineered a path to all or any the nodes then sends the large amount of imitative data packets. These useless data packet exhausts the network resources and thus legitimated user can't able to use the resources for valid communication.

The main influence bring by the attacks against routing protocols include network partition, routing loop; resource deprivation and route hijack [8]. There are some attacks against routing that are studied and documented [10]:

- Impersonating another node to send-up route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence selection to contain other reasonable route messages.
- Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages.

5.6 Denial of Service (DOS)

The first type of attack is denial of service, which aims to crab the accessibility of certain node or even the services of the entire accidental networks. In the conventional wired network, the DOS attacks are accepted out by flooding some reasonably network traffic to the target so as to weaken the processing power of the target and make the services provided by the target become unavailable. However it becomes not sensible to perform the standard DOS attacks because of the mobility and continuously dynamic topology of the mobile. in the mobile accidental networks because of the distributed nature of the services. Moreover, the mobile accidental networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the observation, the attackers exactly use the radio jamming and battery exhaustion strategies to conduct DOS attacks to the mobile accidental networks, which well correspond to the two vulnerabilities.

5.7 Impersonation

Impersonation attack is a severe threat to the safety of mobile accidental network [11]. As we can see, if there is not such a suitably authentication mechanism between the nodes, the human can capture some nodes in the network and arrange them emerge like benign nodes. In this way, the compromise nodes can be a part of the network as the normal nodes and initiate to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

6. PREVIOUS WORK DONE IN FIELD OF ATTACK

Let's look out various researches already done by various researchers.

In this paper [12], project led attacker detection idea for reactive jamming attacks in the deliberate wireless accidental networks. In the most terrible position of interaction, jammers possess the potential to entirely block data transmissions in the wireless network. Since tactical networks are generally utilized in crisis-management and field operations, trust worth and secure communication is a critical issue for mission success. Thus, jamming attacks must be detected and mitigated right away by the wireless network. New approaches for the detection and mitigation of jamming attacks are needed, particularly for tactical networks based on mobile accidental technology where centralized detection algorithms are impractical. We present a new mechanism to discover jamming in tactical accidental networks, which relies on the required number of re-transmission try of transmitted packets and packet delivery rate of received packets. Our predictable approach employs network performance parameters, which differentiate our approach from most existing detection algorithms, since solely a single parameter is usually used as a detection decision.

In this study [13] protocols that will reply to communication disturbance on-demand. In particular, a source node selects multiple different paths for reaching the destination in advance. The availability history of paths are efficiently recorded and calculated via "availability history vectors". Leveraging AHVs, we've get presented two AHV-based multipath selection algorithms: one selects multiple paths through the complete information of AHVs in the network, and the other computes the path in a distributed manner. AHV-based algorithms can effectively identify multiple paths that provide high end-to-end accessibility, even in the presence of a new jammer that did not distress the network before path selection. Additionally, the proposed distributed AHV-based method accomplish higher availability than AODV at a smaller communication cost for lasting communication session

In this paper [14] we proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspect of trustworthiness, namely, social trust and QOS trust.

We developed a probability model utilize stochastic Petri nets techniques to explore the protocol performance, and validated subjective trust against intent trust obtained based on ground truth node position. we incontestable the feasibility of dynamic hierarchical trust organization and application-level trust optimization design concepts with trust based mostly geographic routing and trust-based IDS application, by identifying the greatest way to type trust as well as use trust out of individual public and QOS trust properties at runtime to optimize application performance.

Here trust-based IDS procedure away performs traditional anomaly-based IDS techniques in the detection chance while maintaining sufficiently low false positives. The authors [15] discuss the different kinds of security attacks that can be launch easily in MANETs and related solutions needed for ensure network security. This paper implements the secure ad hoc on-demand distance vector routing protocol (SAODV) and compares the performance of protocol with accessible AODV protocol in the presence of black hole attack. Since public key cryptography is used in this format, it takes essential amount of time to compute digital signature at each node. Besides, this leads to high transparency and processing power requirements.

In this paper author proposed FACES (Friend-Based Ad-hoc routing using challenge to establish Security) [16], that provides a list of trusted nodes to the source node by causation challenges and sharing friend lists. Based on the extent of successful information transmission and therefore the forthcoming relationship with alternative nodes in an exceedingly network, the nodes within the friend lists are rate. The trust level of every node varies from -1 to 4. The nodes within the network are placed in one among the 3 lists, i.e. punctuation mark list, friend list and unauthenticated list. The constant flooding of dispute packet and sharing of friend lists will increase the management transparency.

In this paper [17] author projected per-IP traffic behavioral analysis, during this they gift a period of time DDOS attack discovery on and bar system which might be deployed at the leaf router to watch and detect DDOS attacks. The benefits of this technique inhabit its statelessness and low computation overhead, that makes the system itself support against flooding attacks. Based on the synchronization of TCP and UDP protocol behavior, this technique periodically samples each single informatics user's causation and receiving traffic and judges whether or not its traffic behavior meets the synchronization or not. A brand new statistic CUSUM rule is applied to discover SYN flooding attacks. Moreover, this technique will acknowledge attackers, victims and traditional users, and filter or forward informatics packets by suggests that of a fast identification technique. It has 3 blessings shown as follows.

- Per-IP traffic behavior analyses, it's supported easier to differentiate the attackers from the conventional users.
- As a result of our approach desires less computation and memory, the system might be deployed for on-line DDOS detection and prevention.
- By applying the non-parameter CUSUM rule and call rule, this technique will discover attacks accurately at the faster attack stage.

Moreover, this technique will quickly filter the attack traffics and forward the conventional traffics at the same time by suggest that of the quick identification technology.

During this [18] analysis, rejection of Service attack is applied within the network, evidences are collected to style intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to request out the accuracy of detection engine by discrimination support machine. Universal Detection Engine can generate the friend list in keeping with trust level, higher the trust level of the node is also used for alternative completely different processes like routing, and deciding the cluster head for climbable ad-hoc networks. Part eliminates for Routing parameters and MANET Traffic generation parameter is used for various routing protocols.

7. EXPECTED WORK AGAINST JAMMING ATTACK

Jamming of link between the nodes could cause severe damage, constant fails whole of the network. In proposed work we create a new protection scheme against misbehavior of nodes. In this method first explore the routing behavior of malicious nodes against the behavior of electronic countermeasures attack then concern the appropriate well planned security scheme on it that block the whole misbehavior of malevolent nodes and enhance the network performance. The steps of identify jamming attack are:

- Calculate the number of paths established through multipath routing protocols.
- Check the proper packet delivery in every link that has deliver data to destination.

We will propose a new robust rate adaptation scheme that is resilient to electronic countermeasures attack in a wireless multi-hop deliberate network.

8. CONCLUSION & FUTURE WORK

In Mobile ad hoc Network security is one between the main concerns in case of routing. The secure data communication is necessary for deliver the actual information in right way to receiver. The different types of attack and behavior are observe during this synopsis and also discuss the some scheme against different attack but the electronic countermeasures attack security schemes are mainly focus on this research. In this study, we used the AOMDV routing protocol. But the other a variety of routing protocols could be replicated also. In this paper, we try to resolve electronic countermeasures attack effect in the network. But the detection of this attack is additionally a future work that has simulated in future. Our solution looks the multipath in the AOMDV level. Finding the attacker nodes with connection oriented protocols could be different work as for a future study.

In our future work, we might hold this approach in maximizing the performance of a network from electronic countermeasures attack in term of flooding packets in network by that the link are congested. We simulated attack in the ad-hoc networks and find its affects.

9. REFERENCES

[1] S. Madhavi, “An Intrusion Detection System In Mobile Ad hoc Network”, International Journal of Security and Applications, Vol. 2, No. 3, pp. 1-16, July 2008.

[2] V. P. and R. P. Goyal, “MANET: Vulnerabilities Challenges Attacks Application”, IJCEM International journal of process Engineering & Management, Vol. 11, pp. 32-37, January 2011.

[3] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, “Analyzing the Energy utilization of Security Protocols”, Departure on of International conference of Low Power Electronics and Design (ISLPED ’03), 2003.

[4] Elizabeth M. Royer and Chai-Keong Toh, “A analysis of existing Routing Protocols for ad hoc Mobile Wireless Networks”, IEEE pathetic Communications, Vol. 6, No. 2, pp. 46-55, April 1999.

[5] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of a variety of Routing Protocols for MANETS”, International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[6] S. Ali Dorri, Seyed Reza Kamal and Esmail Kheyrkhah, “Security challenges in Mobile Ad-hoc Networks: A Survey”, International Journal of Computer Science and Engineering Survey (IJCSEC), Vol. 6, No. 1, pp. 15-29, February 2015.

[7] M. Mukesh and K.R. Rishi, “Security characteristic in Mobile ad hoc Network (MANETs): Technical Review”, International Journal of computer Applications, Vol. 12, pp. 37-43, December 2010.

[8] Yongguang Zhang and Winke Lee, "Security in Mobile Ad-Hoc Networks", in volume ad hoc Networks technologies and Protocols (Chapter 9), Springer, 2005.

[9] P. Yi, Z. Dai, S. Zhang, Y. Zhong, "A New Routing Attack In Mobile ad hoc Networks", International Journal of information technology, vol. 11, no. 2, pp. 83-94, 2005.

[10] P. Papadimitratos and Z. J. Hass, "Secure routing for Mobile ad hoc Networks", in measures of SCS Communication Networks and Distributed Systems model and Simulation Conference (CNDS), san Antonio TX, January 2002.

[11] Amitabh Mishra and Ketan M. Nadkarni, "Security in Wireless ad hoc Networks", in volume the instruction book of ad hoc Wireless Networks, CRC Press LLC, 2003.

[12] Aleksi Marttinen, Alexander M. Wyglinski and Riku Jantti, "Statistics-based jamming Detection algorithm for jamming Attacks Against considered MANETs", IEEE Military Communications Conference, pp. 501-506, 2014.

[13] Hussein Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, Member, IEEE, and Adrian Perrig, "Jamming-Resilient Multipath Routing", IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 6, pp. 852-863, November/December 2012.

[14] Detection", IEEE Transactions on Network and S Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho, "hierarchical dependence Management for Wireless sensor Networks and its Applications to Trust-Based Routing and Intrusion ervice Management, Vol. 9, No. 2, pp. 169-182, June 2012.

[15] Preeti Sachan, Pabitra Mohan Khilar, "Security Attacks and solution in MANET", Proceedings of International Conference on Advances in computer Engineering, pp. 172-177, 2011 ACEEE.

[16] Pravina Dhurandher, "FACES: Friend based ad hoc Routing with challenge to establish security in MANET Systems", IEEE SYSTEMS Journal, Vol. 5, No 2, pp. 176-188, June 2011..

[17] Yi Zhang, Qiang Liu, "A Instant DDOS Attack Detection and prevention System support per-IP transfer behavioral Analysis", 3rd IEEE International Conference on Realistic Science and Information Technology (ICCSIT), pp. 163–167, 2010.

[18] Husain, Shahnawaz, Gupta S. C. Chand Mukesh, "Denial of Service Attack in AODV & Friend features mining to design Detection", IEEE International Conference on computer & Communication Technology (ICCCT), pp. 292-297, 2011.