ANALYSIS AND STUDY OF VARIOUS ROUTING VULNERABILITIES IN MOBILE AD HOC NETWORK

Ms. K. KAVYA, Dr. N. SHANMUGA PRIYA
Research Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
Associate Professor & Head, Department of Information Technology, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore.

Abstract: A MANET incorporates of a group of hosts that shape an arbitrary network topology via any of numerous wireless conversations medium. It is apparent that the routing MANET is intrinsically amazing from traditional routing located on a infrastructure networks. Routing in a MANET is predicated upon on many factors which include topology, selection of routers, initiation of request, and specific underlying characteristic that might function a heuristic in finding the route rapid and efficaciously. In any sort of community the routing is the best hassle to be treated. Message protection plays most crucial importance in cell ad-hoc networks however wireless networks are at risk of many attacks that aren't secured and plenty less-worth. The intermediate nodes cooperate with each specific as there can be no such base station or access factor. The routing protocols play essential function in shifting information. Trust mechanism secures records forwarding via isolating nodes with malicious intention using believe charge on the nodes. In this paper, the severa consider primarily based routing scheme to enhance the routing overall performance and first-class of provider of the MANET.

Keywords: *Ad hoc Network, Routing, Trust Scheme, Quality.*

I. INTRODUCTION

MANET (Mobile Ad-hoc Network) is a famous and widely used wireless community. MANET is a kind of self-organizing and decentralized machine. It is a network crafted from numerous wireless cell nodes which collectively work together just so transmission is viable among any of the nodes in the machine. Nodes talk with every extraordinary with the direct shared wireless radio links. All the cellular hosts act as routers in the network. Due to open and dynamic nature, this network is quite at risk of amount of attacks. Information in the form of packets is transmitted from supply to vacation spot with the assist of various nodes within the path [1]. There are positive subjects which ought to be observed as Route choice, Request initiation, topology used and so forth. Trust is defined as a diploma of perception amongst numerous entities. They consider for equal entity can be unique while evaluated with the aid of distinctive humans. Trust control is a gadget in an effort to guarantee various crucial features like security, get admission to manage, intrusion detection, keeping apart malicious nodes and so on. During conversation, a selfish node to save its resource, does no longer cooperate and even drops the packet. To avoid this, reputation mechanisms are used. A popularity is defined as an import of the beyond behavior of an entity. The recognition machine keeps a blacklist which incorporates the records of malicious nodes. Malicious nodes purpose numerous attacks like Black hollow assault and cooperative black hollow for which a Trust based totally technique is used. In this accept as true with cost related to every node that is represented with the trustworthiness to each of its neighboring nodes is calculated. Communication in mobile ad hoc networks incorporates two stages, route discovery and statistics transmission. In a destructive environment, both phases are liable to a ramification of attacks. First, misbehaving nodes can disrupt the route discovery through impersonating the vacation spot, by way of responding with stale or corrupted routing statistics, or by means of disseminating forged control site visitors. This manner, attackers can impede the propagation of legitimate route manage visitors and adversely have an impact on the topological understanding of benign nodes. However, misbehaving nodes also can disrupt the facts transmission segment and, hence, incur good sized facts loss by means of tampering with, fraudulently redirecting, or even losing records visitors, or injecting cast statistics packets. The main capabilities and characteristics of MANET [1] are:

1. Cooperation: - In MANET cooperation of nodes is needed while a node desires to speak with a node that is out of its variety. In this example, a valid, at ease, highest quality direction is needed for the verbal exchange. To locate this sort of direction cooperation of intermediate nodes plays a vital position. Without cooperation of nodes it would be by no means feasible to speak with out of range nodes.

2. Dynamic topology: - The behaviour of nodes inside the MANET is unpredictable, common and random in nature. The nodes can leave or join the network at any time which makes routing very difficult. Due to this randomness of nodes, the

topology of the network can trade at any time which creates a huge assignment in MANET layout.

3. Resource Constraints: - MANETs are produced from cellular nodes which have confined assets like battery electricity, bandwidth, low computational potential and so on. So to acquire dependable communique these aid constraints make the project more enduring.

II. LITERATURE REVIEW

A MANET contains of a group of connecting hosts that structure an arbitrary community topology via any of several wireless communique medium. MANET communications characterize a diversification in verbal exchange generation crucial to solve the stringent cease-to-stop necessities of QoS-primarily based conversation networks.

The rising generation of MANET is based totally on wireless multihop architecture without constant infrastructure and prior configuration of the community nodes.

Jhaveri et al. proposed a composite consider model which applied each social and QoS accept as true with components [1] to estimate the agree with diploma of nodes wherein the trench ratio became used as a social accept as true with thing. This ditch ratio parameter is treasured for knowing the behavior of nodes and to pick out malicious nodes. In the paper, energy intake was described as an factor of QoS through considering the ratio of packet drop of a selected node. Nodes with the lowest stage of strength are considered as un-depended on nodes. The proposed scheme confirmed a few enhancements in packet transport ratio when in comparison to some different methods.

Rajkumar et al. proposed a Certificate distribution and a Trust based totally threshold revocation technique [2]. In this work, the authors developed a believe-based solution using an green mechanism for certificates revocation and validation by using combining public key certificate, so that it will decorate the safety of the network by using decreasing the hazards from malicious nodes. Initially, the trust values had been derived from the direct and oblique agree with values and the secret key to all of the nodes were distributed via a certificates authority. Followed by way of this, a accept as true with based threshold revocation method is computed. Here the misbehaving nodes are eliminated.

Cho et al. proposed a composite agree with-based totally public key management (CTPKM) method with an idea of maximizing the overall performance of network at the same time as mitigating the vulnerabilities. Based on the concept of agree with, the proposed technique adopts absolutely distributed believe-primarily based public key management primarily based policy for MANETs using an smooth protection mechanism [3]. This work goals to maximize performance by way of using consider-based totally method, instead of using hard security parameters to get rid of safety vulnerabilities. During the routing process, the nodes determine the trust of every other node using a trust threshold. The results depict that CTPKM minimizes the hazard at a huge margin using an gold standard consider threshold and maximizes the service availability with ideal conversation overhead received through trust and key control operations.

Sanaz Farajzadeh, PeymanKabiri, (2016) Proposed trust version is primarily based on Bayesian model and makes use of watchdog to get admission to packets that aren't forwarded through the nodes. Ad hoc networks are demonstrated to be vulnerable to special types of attacks, given the ease of the way malicious nodes can infiltrate them. Since these networks lack central manipulate and predetermined topology or infrastructure and they are clean to implement. Hence, they are appropriate desire in emergency and accessions which include remedy or military operations. Topology of those networks is continuously converting, nodes act autonomously and their location can change at any time [4].

Jan Papaj and LubomirDobos, (2016) proposed models are primarily based on the direct model for the agree with computation. Models also are based totally on the belief that every node in the community gets information approximately different nodes. The proposed set of rules is running on the community layer of the MANET layer model and is designed for gathering of the routing and information node information throughout the complete operations certain for the routing. The Mobile Ad Hoc Network (MANET) is characterized by multihop communique between cellular nodes by using wireless. The hybrid MANET-DTN also requires the cooperation among cellular terminals which will make a spread of the relay nodes [5].

III. VULNERABILITIES OF MANET

Vulnerability is a weak spot in protection system or Wireless System. A unique system may be liable to unauthorized statistics manipulation due to the fact the machine does no longer confirm a person's identification earlier than permitting facts get admission to. MANETs is extra vulnerable than wired community. Some MANETs vulnerabilities are as follows [1][7]:-

- **Wireless Links:** First of all, the usage of wireless links makes the community susceptible to attacks including eavesdropping and energetic interference. Unlike wired networks, attackers do not want physical access to the community to carry out those attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can make the most this selection, consuming community bandwidth easily to save you normal communication among nodes.
- **No predefined Boundary:** In MANETs, we can't exactly outline a bodily boundary of the networks. The nodes work in a nomadic surroundings where they may be

allowed to sign up for and depart the wireless community. As quickly as an adversary comes inside the radio range of a node it'll be able to communicate with that node.

- **Scalability:** Due to mobility of nodes, scale of advert-hoc community converting all of the time. So scalability is a prime difficulty concerning protection. Security mechanism should be able to handling a huge network as well as small ones.
- **Resource availability:** Resource availability is a chief problem in MANETs. Providing relaxed verbal exchange in such converting surroundings as well as safety towards specific threats and attacks, results in improvement of diverse safety schemes and architectures. Collaborative advert-hoc environments also permit implementation of self-organized security mechanism.
- **Lack of Centralized Management Facility:** Ad hoc networks do no longer have a centralized piece of management machinery which includes a name server, which cause a few vulnerable troubles. Now let us talk this problem in a more distinct way First of all, the absence of centralized management machinery makes the detection of attacks a totally hard trouble because it isn't always easy to display the visitors in a exceedingly dynamic and huge scale ad hoc network. Second, lack of centralized control machinery will postpone the believe management for the nodes inside the advert hoc network. Third, essential algorithms inside the mobile ad hoc network depend upon the cooperative participation of all nodes and the infrastructure. Because there may be no centralized authority, and selection-making in mobile ad hoc network is every now and then decentralized, the adversary can employ this vulnerability and carry out some attacks that can ruin the cooperative set of rules.
- **Cooperativeness:** In MANETs, all routing protocols assume that nodes provide relaxed communique. But some nodes may additionally emerge as malicious nodes which disrupt the network operation by means of changing routing data and so forth.
- **Infrastructure much less:** MANETs is an infrastructure much less community, there's no principal administration. Each tool can talk with every different device, hence it will become tough to hit upon and control the faults. In MANETs, the mobile devices can circulate randomly. The use of this dynamic topology effects in course adjustments, common network walls and likely packet losses.
- **Limited strength supply:** The nodes in cell advert-hoc community need to consider constrained power deliver, so as to cause numerous issues. A node in mobile ad-hoc network might also behave in a selfish way while it's far finding that there's only limited energy supply.
- **Dynamic topology:** Dynamic topology and changeable nodes club may additionally disturb the trust relationship amongst nodes. The consider may also be disturbed if a few nodes are detected as compromised. This dynamic behavior can be higher included with allotted and adaptive safety mechanisms.
- **Bandwidth Constraint:** Variable low potential hyperlinks exist in comparison to wireless community which are extra at risk of outside noise, interference and signal attenuation results.
- **Adversary in the Network:** The mobile nodes inside the MANETs can freely join and depart the community. The nodes within network may additionally behave maliciously. This is hard to discover that the behavior of the node is malicious. Thus this assault is greater dangerous than the external assault. These nodes are known as compromised nodes.

IV. ROUTING ATTACKS AGAINST MANET

Attacks in the ad-hoc network are of kinds passive assault and active attack. Passive assault occurs which disrupt the operation of the community that means it does now not regulate the content material statistics. This sort of attack is less dangerous but greater complex to find as it does interfere with operation. To triumph over this a few powerful encryption approach can be used to encrypt the facts whilst transmission. In comparison, lively attack is one that actively modifies, modify and break the facts being transmitted, for this reason disrupting the statistics change. Active attacks can be categorised as External attack and inner attacks. External attacks come from the node which does belong to the a part of the community. This can be averted through some safety mechanism which includes encryption and firewall. Internal attacks will carried out from in the community. These attacks are extra severe and hard to detect.

The malicious node(s) can attacks in MANET using distinct methods, together with sending faux messages numerous times, fake routing records, and advertising and marketing faux hyperlinks to disrupt routing operations. We've got categorized the currently existing attacks into two vast categories: DATA site visitor's attacks and CONTROL visitors attacks. This class is primarily based on their commonplace traits and attack goals. For instance: Black-Hole assault drops packets whenever, at the same time as Gray-Hole attack also drops packets but its action is based on conditions: time or sender node. But from community point of view, each attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack whilst it starts dropping packets. So they may be categorized below a single class.

A. Data Traffic Attack & Control Traffic Attack

Data traffic attack deals both in nodes losing data packets passing via them or in delaying of forwarding of the information packets. Some forms of assaults select victim packets for losing at the identical time as a number of them drop they all regardless of sender nodes. This can also moreover substantially degrade the splendid of carrier and will increase give up to give up put off. This additionally causes large loss of vital records. For e.g., a 100Mbps wireless hyperlink can behave as 1Mbps connection. Moreover, except there is a redundant path around the erratic node, some of the nodes may be unreachable from every other altogether.

Mobile Ad-Hoc Network (MANET) is inherently liable to attack due to its essential characteristics, which include open medium, allotted nodes, autonomy of nodes participation in community (nodes can be a part of and leave the network on its will), loss of centralized authority which can put in force protection at the community, disbursed co-ordination and cooperation. The existing routing protocols cannot be used in MANET because of those reasons.

Though there may be other kinds of assault, together with jamming attacks, which is not CONTROL attack. They may be tackled as part of bodily layer security protocols.

B. Black-Hole Attack

This is an internal attack in which an attacker advertises it as having a shortest and clean route to destination fooling all nodes round it. A malicious node first sends fake routing information, claiming that it has an ultimate direction and causes different nodes to direction facts packets thru the malicious one [7]. Thereafter, malicious node drops all the obtained packets instead of forwarding the ones packets typically within the community.

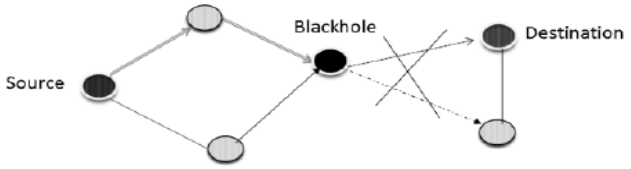

Fig 1: - Black Hole Attack

Here the Black-Hole node separates the network into two elements. Few techniques to mitigate the trouble: (i) collecting multiple RREP messages (from extra than two nodes) and thus hoping more than one redundant path to the vacation spot node and then buffering the packets till a safe path is located. (ii) Maintaining a desk in every node with previous sequence range in increasing order. Each node before forwarding packets will increase the series number. The sender node proclaims RREQ to its pals and once this RREQ reaches the vacation spot, it replies with a RREP with ultimate packet series number. If the intermediate node unearths that RREP contains a wrong sequence wide variety, it knows that somewhere something went wrong.

C. Worm-Hole Attack

A computer virus-hole assault is a critical and excessive attack in MANET. In this assault, an attacker captures every manage packet in advert-hoc network and tunnels it to every other malicious node. This attack disrupts the everyday routing with the aid of developing the illusion that end-nodes of wormhole tunnel are pals but in fact they not. This assault is difficult to locate. In the fig. Malicious nodes M and N create a false tunnel to forward the packet to be able to tamper the statistics packets and disrupt the routing technique.

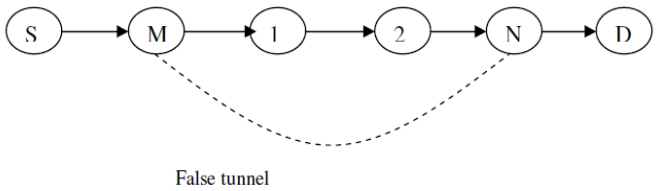

Fig 2: - Worm-Hole Attack

D. Gray-Hole Attack

In "Grey Hole Attack", [6] the malicious node first captures the route as in Black hole attack with the aid of exploiting the vulnerabilities of direction discovery system of the routing protocols and then it drops the intercepted packets with a positive chance. The malicious node on this kind of assault might also drop packets coming from positive particular nodes at the same time as forwarding all of the packets for other nodes or it can drop packets for some time and behave usually for relaxation of the time or a mixture of the above , thereby making detection of malicious node very difficult. Fig. 2 shows the Gray Hole Node (GHN) drop the packets coming from the target node.

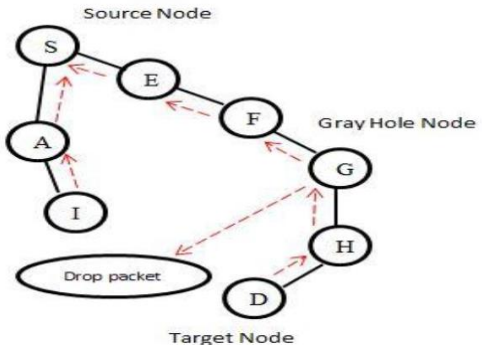

Fig 3: - Gray-Hole Attack

E. Sybil Attack

In "Sybil Attack" [9] [10] a malicious node creates and controls a couple of identities. A node inside the community is recognized via a completely unique identifier (address) and there's one-to-one mapping between the node and the identification. Two different identities constitute extraordinary nodes. MANETs do no longer have any centralized identity control mechanism as a consequence a malicious node can assume multiple identities and might create several digital nodes by way of assuming new identities. The Sybil assault may be launched in ways, within the first case a malicious node creates a brand new identity after discarding the previously created identity and consequently one identification of attacker is lively at one time. The goal of such attack is to delink the malicious node from its in advance malicious sports. In the second one case the malicious node assumes several identities concurrently with the purpose to cause disruption inside the community.

F. Flooding Attack

In "Flooding Attack" [11] the attack is released by way of flooding of RREQ message in the reactive routing protocol. A malicious node can flood the community with route request to the nonexistent or arbitrary destinations. The reason is to unnecessarily use bandwidth, computational sources, reminiscence resources, energy sources, and forestalls the normal operation of the routing-protocol. In proactive protocols flooding of the TC message will motive such an assault. As those protocols create and keep routes to all different nodes inside the community thru exchange of TC messages, whose rate is not managed, these are greater at risk of such attacks.

V. CONCLUSION

In this paper, we have analyzed the routing technique, their vulnerabilities and the various forms of attacks which may be launched via exploiting the same, to disrupt the routing manner or release DoS attacks. In this paper we addressed current capability safety threats in MANETs. In this examine we located that maximum of the work on MANET protection targeted on single layer assaults i.E. Active and passive attacks. In the in the meantime a few assaults related to more than one nodes have obtained little interest due to the fact that they're surprising and blended attacks i.E. Collaborative assaults. There were no right definition and categorization of these kinds of collaborative assaults in MANETs. Thus, protection of verbal exchange machine towards these sorts of attacks is a tough assignment. Development of a multi-fence safety solution this is embedded into probably every element inside the community, ensuing intensive protection that offer multiple line of defense against many recognized and unknown protection threats is also given importance. Further, there is additionally a want to broaden a detection and protection mechanism for coping with messages in comfortable way.

VI. REFERENCES

[1]. Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. In Ad Hoc Netw.; Ortiz, J.H., de la Cruz, A.P., Eds.; InTech: London, UK, 2017; ISBN 978-953-51-3109-0.

[2]. Rajkumar, B.; Narsimha, G. Trust Based Certificate Revocation for Secure Routing in MANET. Procedia Comput. Sci. **2016**, 92, 431–441. [CrossRef]

[3]. Cho, J.-H.; Chen, I.-R.; Kevin, S.J. Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Netw. **2016**, 44, 58–75. [CrossRef]

[4]. Sanaz Farajzadeh, Peyman Kabiri, "Trust Based Secure Route Detection for MANETs", Journal of productivity and development 3(1) 2017:13-25 www.pdjour.com.

[5]. JanPapaj and LubomirDobos, "Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 7353691, 18 pages http://dx.doi.org/10.1155/2016/7353691.

[6]. Sowmya P, V. Anitha, Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014.

[7]. F.R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hocnetworks," EURASIP Journal on Wireless Communications and Networking - Special issue on wireless network security, 2013.

[8]. D. Helen and D. Arivazhagan, "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014 (ISSN: 2278-5213)

[9]. Meenakshi Yadav1 , Nisha Uparosiya2, "Survey on MANET: Routing Protocols, Advantages, Problems and Security",International Journal of Innovative Computer Science & Engineering,2014 (ISSN: 2393-8528).

[10]. Chavda, K. et al., "Removal of Black Hole Attack in AODV Routing Protocol of MANET", 4th ICCCNT, Tiruchengode, July 2013.

[11]. Howarth, M. P. et al., "A survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, 2013.

[12]. GAYE Abdourahime, Dr Karim KONATE: Attacks analysis and countermeasures in routing protocols of mobile ad hoc networks,COMPUSOFT, An international journal of advanced computer technology (IJACT),ISSN: 2320 – 0790, December 2014.

[13]. Cai Y, Xu X, He B, Yang W, Zhou X. Protecting cognitive radio networks against poisson distributed eavesdroppers. In: International Conference on Communications ICC; Kuala Lumpur, Malaysia; 2016.

[14]. Marinho J, Granjal J, Monteiro E. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP J Inf Secur*. 2015:1-14.

[15]. Prabhleen Kaur, Sukhman, " An Overview on MANET-Advantages, Characteristics and Security Attacks", International

Journal of Computer Applications (0975–8887), 4th International Conference on Advancements in Engineering & Technology (ICAET 2016).