Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Mobile Ad-hoc Networks (MANETs) Routing Prerequisites Including Prevention/Avoidance of Selfish Nodes Attack on Network Layer: A Detailed Case Study

Snehil Gautam
Department of ECE, KITM,
Kurukshetra University, India

Ritesh Goel
Department of ECE, K ITM,
Kurukshetra University, India

Nitin Goel
Patent Analyst, MSPE,
Noida, India

Abstract- Mobile ad hoc networks (MANETs) are a kind of network that has no centralized body to communicate with the nodes. It has no fixed topology. Also it is difficult to find the route from source to destination in MANETs, because of its arbitrary mobility of nodes and in general MANETs works on multihop environment. We present a classification of routing protocols and their brief description, based on their operating principles and underlying features. The clustering algorithms with time and message complexities that are possibly low and independent of the total number of nodes in the network are crucial for the design and operation of very large scale wireless mobile ad hoc networks (MANETs). This paper discusses a cluster based selfish node schemes and algorithms for mobile ad hoc networks (MANETs). An efficient clustering strategy which considers the attacks under network layer and mitigate non-legitimate node scenario, can improve the performance of flexibility and scalability.

Keywords - MANET, Selfish Nodes, Man-in-the-middle attack(MITM) , Multi-hoping

I. INTRODUCTION

Extending mobility into self organized and wireless domains is the main objective of MANET, where a set of nodes form the network routing infrastructure in an ad hoc fashion having self monitoring capabilities**.** MANET offers a friendly and co-operative environment with no centralized place where traffic monitoring or access control mechanism can be deployed. Unlike the wire line networks it poses some unique characteristics such as shared wireless medium, stringent resource constraints, highly dynamic network topology, and peer to peer and multihop autonomous network architecture. From the security design perspective, the lack of a clear line of defense is one of the distinguishing characteristic. The network connectivity between the nodes in MANET is provided over potentially multi-hop wireless channel mainly through link layer protocols that ensures single hop connectivity and network layer protocols that extend the connectivity to multiple hops. But the multi-hopping capabilities of these MANETs suffer in the case where a large number of nodes are operational, triggering a deterioration in the network's performance. [1]

In MANETs every node may function as a router and forward packets through routing paths. Co-operation among nodes during path discovery and packet relaying is of primary concern for correct functioning of the network. Communication in a MANET occurs in a discrete and disperse environment with no centralized management which arises a main issue in MANET that is the breakage of link at certain moment and re-generation of link at certain state as it consists of routers which are mobile in nature i.e. are independent to roam in an arbitrary motion.

II. VULNERABILITIES TO NON LEGITIMATE SECURE ROUTING IN MOBILE AD HOC NETWORKS (MANETS) UNDER LAYERD ATTACKS FOR SELFISH NODES

A. Link unreliability: The correct operation of the network requires not only the correct execution of the network functions but also some schemes to cope up with dynamically changing network topology. A link no longer participates in a packet forwarding process because of its corresponding node movement and limited resources which causes havoc in the network as the routing suffers an interruption, nodes have to retransmit the lost packets, and network has to reconfigure the path to the destination.

Solution: Computation of link reliability as safe or unsafe. The havoc caused by several link breaks can be controlled, if its reliability is estimated and a trust level is associated accordingly.To implement this idea, a node must be issued with an off-line certificate by several other nodes in the network, on the basis of its behavior like its mobility and resource availability.

B. Bandwidth constraints: The networking scenario in mobile ad hoc wireless network is distributed in nature.In such environment the optimal utilization of the bandwidth among nodes is not expectedly supported.

Solution: Adaptive protocols. To countermeasure the effects caused by the bandwidth constrained ad hoc network,Forwarded data packet is embedded with some information regarding the bandwidth it requires for its relaying and processing. The intermediate/destination nodes check this requirement and then take an action accordingly.

C. Resource Limitation: Various routing, packet forwarding, service discovery and security schemes adopted by each device in the network has to work within its own resource limitations in terms of computation capabilities, memory,

ommunication capacity and energy supply. The battery power/energy carried by a mobile node has limited energy and processing power which leads to the support for limited number of applications and services.

Solution: Reduce the overhead. The scarcity of resources within a network causes denial of services, which can be overcome by enabling a node to set a threshold value for its processing power, battery, communication capabilities and other resources. When a node receives a packet, it checks its threshold limit, if the node does not find itself able to process that packet; it chooses some of its neighbor nodes to process that packet. It maintains a queue, when data traffic is high in the network.

D. Route maintenance: Mobile hosts in mobile ad hoc network usually move freely, which causes the topology of the network to change dynamically and disconnection occurs frequently. The nodes take advantage of the multihoping nature of the mobile ad hoc network and search for an alternative path to the destination for the data transfer. But the data sent by the source node during alternate path establishment period will be lost leads to incomplete data transfer and thus become responsible for a considerable increase in network traffic because of the retransmission of the data after re-establishing the link.

Solution: Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates to other nodes in the network. If the status of a link or a node changes, the periodic updates will eventually reflect the changes in all other nodes presumably resulting in the computation of the new routes to the destination nodes. The route maintenance approach adapted by the preemptive routing scheme involves the routing algorithm to discover an alternative path before the breakage of the actual link. Thus improves the network connectivity.

E. Network partition: The routing protocols being implemented in adhoc environment sometimes do not cope with network partitions. This sort of partitioning affects the performance badly and has severe consequences which includes non optimal routes and loss of data etc.

Solution: Network partition mainly occurs due the node movement and thus the other nodes which were connected to this 'moved away' node suffers a disconnection with the rest of the network. The connection can be again established through periodic sending of beacon messages or through predicting the node movement and link breakage.

F. Hidden Terminal Problem: The data transmission from sender to receiver, sometimes suffers a sudden interruption collision due to the simultaneous transmission from these nodes, which are not within the direct transmission range of receiver. These nodes are considered as the hidden nodes. The shared wireless link does not allow this type of transmission to take place which results in collision and packet loss. Hidden terminal problem degrades the system performance and throughput and needs to be alleviated.[6]

Solution: The collision among data packets during the transmission from the hidden nodes can be avoided if a priority assigning scheme is employed with in the network for various cells to which the communicating nodes belong. When a node receives the data packets from other multiple hidden nodes it checks the priority or preference level of the cell this sending node belongs to and acknowledge it accordingly. Thus this priority wise servicing of multiple hidden nodes can eliminate the chances of collision among the packets.

G. Exposed terminal problem: Exposed terminal problem prevents a node from transmitting data when a nearby node (in the direct transmission range) occupies the wireless channel to transmit packets to the destination node. The alleviation of this problem needs some synchronization mechanism to be established among the nodes in the network, so that the throughput cannot be affected during high traffic loads. Nodes overhear the channel and starve themselves until the other node which belongs to the same cell as that of the overhearing nodes continue transmitting packets.

Solution: Exposed nodes, if assigned a priority or preference by the receiving node, can alleviate this problem. The receiving node makes a check over the priority of the sending node and acknowledges it according to that preference level it is assigned with. So the exposed nodes need not prevent themselves to send data over the shared channel

H. Unpredictable connectivity: If a mobile node in MANET want to transmit data packets to the rest of the network then it requests its neighbor node for their co-operation to detect the routes and then to relay the packet. If a node deny forwarding it then the given source node request some other nearest and node for the same purpose. Moreover the node movement and scarcity of resources at nodes affects the connectivity. This unpredictability in establishing a connection with other nodes results in the delay and the formation of non-optimal paths in the network.

Solution: Integrate Mobile ad hoc networks with Artificial intelligence and neural networks. If a network is made to operate intelligently, which can predict its future connectivity with other nodes on the basis of its learning and training then it would be far more easy for a mobile node to detect its efficient and optimal paths to the destination with no or small delays. Mobility of nodes is the biggest hindrance in the path of network training. The maintenance of broken links, QoS, traffic management, provisioning of security, location discovery, congestion control, measurement of resources etc. can be handled effectively if the network is well trained.

III CHALLENGES TO AD HOC ROUTING

Existing MANET routing protocols faces many problems, such as security and performance. These are describing as follows:-

A. Denial of service (DOS): In DOS, a particular node that contain single or multiple paths passing through it may stop forwarding packets and still maintaining its presence in the network, therefore behave as a sink for data in the network.

B. Black Hole: In black hole attack malicious node replies to every RREQ by falsely claiming that it contain a fresh enough route to the destination. Hence all the traffic of the network is redirected to that malicious node which then dumps them all [6].

C. Rushing: It results in denial-of-service when used against all previous on-demand ad hoc networks routing protocol. In this, attacker relays received route request without any change as soon as possible, by suppressing any later legitimate route request [7].

D. Wormhole: These attacks are hard to detect because the path that is used to pass on information is not part of the actual network. In this, a malicious node uses external path in the network to route messages to other node at other location [8].

E. Selfish: As nodes in MANET have limited resources, especially battery power and bandwidth. Hence some nodes deny to forward or selectively forwarding the packets from other nodes to save its resources.

IV. SECURITY AND TRUST MANAGEMENT IN MANETS

The lack of structured hierarchy in MANETs complicates the overall task of implementing Security policies. The nodes are responsible of not only forwarding packets for other nodes but also perform extensive computation. These computations can be in terms of route maintenance, key management and the deployment of security schemes.

Mobile Ad-hoc Network has the ability to configure and to maintain the network by itself; these are flexible with arbitrary located nodes. In such conditions, the communication through the network demands extra efforts to be employed for the secure transition of packets. The design of an efficient routing protocol that has both strong security and high network performance is an evitable task in such a dynamic multi-hop autonomous network. Wireless network offers communication capability and information access regarding of its location to its users. Security wireless ad-hoc network has become a primary concern in attempt to provide secure and efficient communication and performance in a hostile environment. [14]

Different kinds of ad hoc routing threat models and threats have been pointed out. Several models to external threats in ad hoc environment have also been given with major categories like passive eavesdropping and active interference and similar with the case of internal threats with major categories like failed nodes, selfish nodes and malicious nodes. In this connection by taking the consideration of all kinds of threats with their behavior we are able to understand what could be the probable loophole and vulnerabilities in mobile ad hoc network. Along with that there are some other issues that are directly related to mechanism and simulation design. Of sure while designing a new protocol, we should give more emphasis to these issues.[11]

V. SELFISH OR MISBEHAVIOR DETECTION SCHEMES

The effective operation of mobile ad-hoc networks (MANETs) is compromised by the selfish or misbehaving nature of certain mobile nodes. The inefficiency of a variety of misbehavior detection scheme results in false accusations and is unable to avoid ambiguous collisions, receiver collisions or nodes capable of controlling their transmission power. Detection of packet forwarding misbehavior through principle of conservation of flow judges a node through estimating the percentage of packets dropped which is compared against a pre-established threshold and presents a solution to above problem. This scheme can be implemented in conjunction with various routing algorithm including SRP, ARAN, SEAD etc. Identifying any source(s) that appear to be causing packet losses, allowing for their isolation at a later stage is the objective of this approach. In an ideal static network, the flow conservation principle states that all the amount of packets sent to a node to forward and the amount of packets forwarded by this node to them must be equal. The loss of packets in the network because of the collision and error prone nature of wireless network makes the function far from ideal. A threshold needs to be established to account for packets dropped by a node though no fault of its own i.e. $0 < \alpha\text{threshold} <1$. In a highly dynamic environment, it is highly difficult to determine nodes that have transmitted and received packets from the node under evaluation. A limited broadcast scheme can overcome this problem. A node in the network maintains a table for each node to which it has transmitted packets to or receive packets from and continuously monitor its neighbors and update the list of those it has heard recently. The entry in table of overheard node is updated with a timestamp corresponding to the time the node was last overheard. A node broadcast a metrics request packet (MREQ) with TTL=1 in the IP header when it checks the behavior of a node. To prevent the flooding to traverse more than once, MREQ_ID and a timestamp is included in the request packet. Reply handling is executed at the node which initiated the evaluation of a node by sending MREQ. The replies from all the neighbor nodes are computed to meet the flow conservation equation. So this approach does not require high density networks in which many nodes can overhear each other's received and transmitted packets. If the present scheme is employed in a collaborative manner then the detection can provide better results. The keys which are still to be discovered are the determination of accurate threshold value and the determination of time intervals between successive evaluations so that collisions can be avoided effectively.[4]

VI. A SECURE CLUSTERING SCHEME PROTOCOL FOR MANET

In this protocol, all the nodes within the networks are divided into several clusters. Here the trust value between the nodes is calculated according to their interaction behaviors. Based on the trust value, it can be judged whether the connection between the two nodes is trusted or not. So cluster head can be selected and the nodes which have trust connection with cluster head will be the core nodes. The cluster head and core nodes can join together to be the service group for the cluster.

Each node is expected to contribute to the network on the continual basis within a time frame. Those which fail will undergo a test for their suspicious behaviour.

If it discards the packet and does not respond, the monitoring nodes will label the suspicious node as selfish.

Once one node has been verified as a malicious node, cluster head will broadcast the news to all the cluster members and

refuse to provide updating service for the malicious node. Because of that, the malicious node will be shielded by the cluster forever. The keys of nodes and cluster are generated after consultation among the service group members , Man-in-the-middle attack can be resisted by this way. At the same time, the cluster can achieve the periodic update, the cluster head will be reselected, service group will be reformed, subsequently, the key of cluster and nodes will be updated as well.[16]

VII. PREVENTING ARP POISONING-BASED MAN-IN-THE-MIDDLE ATTACKS

In this paper, an enhanced version of Address Resolution Protocol (ARP) is proposed to prevent ARP poisoning based Man-in-the-Middle (MITM) attacks. When a node knows the correct Media Access Control (MAC) address for a given IP address, if it retains the IP/MAC address mapping while that machine is alive, then MITM attack is impossible for that IP address. In order to prevent MITM attacks even for a new IP address, a voting-based resolution mechanism is proposed. The proposed scheme is backward compatible with existing ARP and incrementally deployable.

A new mechanism to prevent ARP poisoning-based MITM attacks is proposed based on two key concepts: long-term IP/MAC mapping table and voting. Even though the proposed scheme is installed on a small number of hosts, they can be well protected through voting-based collaboration. Since the proposed scheme does not use cryptography and central servers, it does not have complexity and single point of failure problems while achieving backward compatibility with existing ARP.[17]

VIII. CONCLUSION

Prolonged network lifetime, scalability, and selfish node detection are important necessities for numerous mobile ad-hoc network applications. Clustering the MANET nodes,

keeping selfish nodes detection and mitigation of the network in mind is an effective technique for achieving these goals. The objective function formulated to mitigate selfish node problem into an optimization problem achieves the tradeoff between energy efficiency and secure efficient cluster. These solutions only cover a subset of all the vulnerabilities, prevention and detection of selfish nodes which may inject into the network and are far from providing a comprehensive answer to the routing and security problems in MANETs. Beyond proper security it is possible to gain many advantages by malicious behavior. So, by diverting the traffic towards from a node, no forwarding at all, incorrect forwarding, and other non-cooperative behavior, nodes can attack to the network.

REFERENCES

[1]. Hao Yang, Haiyun luo, Fan Ye, Songwu Lu and Lixia Zhanng, “Security on Mobile Ad Hoc Networks: Challenges and Solutions” 1536-1284/04/IEEE Wireless Communications Feb. 2004.

[2]. C.Siva Ram Murthy & B.S Manoj, “Mobile Ad Hoc Networks- Architectures & Protocols” , Pearson Education, New Delhi, 2004.

[3]. Ajay Jangra, Nitin Goel, Priyanka, Komal, “Security Aspects in Mobile Ad Hoc Network (MANETs): A Big Picture”, International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.

[4]. Amit Goel, A.k.Sharma, “Security Trends in Wireless LAN”.

[5]. B. R. Sujatha, M V Satyanarayana, “Improved Network Connectivity in MANETs”, International Journal of Computer Networks & Communications (IJCNC),Vol.1,No.3,October 2009

[6]. Santhosh Krishna B.V, Mrs. Vallikannu A.L, “ Detecting Malicious Nodes For Secure Routing in MANETs Using Reputation Based Mechanism”, Published in International of Scientific & Engineering Research, Volume 1, Issue 3, December 2010.

[7]. Y.C.Hu,A. Perrig and D.B Johnson, “Rushing attacks and defense in Wireless ad hoc network routing protocols,”, in proceddings of the ACM workshop on Wireless Security, pp. 172-194, ACM, September 2003.

[8]. Y.C. Hu, A. Perrig and D.B. Johnson, “Packets leashes: a defense against wormhole attacks in Wireless networks”, in proceddings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Soieties, vol. 3, pp. 1976-1986, San Francisco, Calif, USA, March-April 2003.

[9]. E.Venkat Reddy, “ Trustworthy Robust Routing Protocol for Mobile Ad hoc Network”, Amina Institute of Technology, Hyderabad, Andhra Pradesh-India, Published in E. Venkat reddy/ International Journal Of Engineering Science and Technology Vol.2 (2), 2010,77-86. Xie Hai-tao, “A Cluster-Based Key Management Scheme for MANET”, ©2011

[11] Vikas Kawadia and P. R. Kumar, “Power Control and Clustering in Ad Hoc Networks”, ©2003 IEEE.

[12] Calafate, C.T. Cano, A QoS architecture for MANETs supporting real-time peer-to-peer multimedia applications, ©2006 IEEE.

[13] Vinh Pham, Erlend Larsen,“A Radio load Based load Balancing Scheme with Admission Control”, ©2011 IEEE.

[14] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, “ A Survey of Secure Mobile Ad Hoc Routing Protocols”, 1553-877X/08/IEEE 2008.

[15] Seung Yi, Robin Kravets “MOCA: Mobile Certificate Authority for Wireless AdHoc Networks” University of Illinois at Urbana-Champaign Urbana,IL61801, {seungyi,rhk}@cs.uiuc .edu.

[16] Li Wang, Fei Gao "A Secure Clustering Scheme Protocol for MANET"© 2010 IEEE

[17] Seung Yeob Nam,Dongwon Kim, and Jeongeun KimEnhanced "ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks "© 2010 IEEE

