A REVIEW: SECURE AND RELIABLE ROUTING IN MANETS WITH THE DETECTION AND PREVENTION OF SELFISH ATTACKS

Divyeshkumar Jayantibhai Hariyani[1], Munindra Lunagaria[2]

[1]Reaserch Scholar, Department of Computer, Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat, India
[2] Assistant Professor, Department of Computer, Marwadi Education Foundation's Group of Institutions Rajkot, Gujarat, India

---

ABSTRACT: *A mobile ad hoc network (MANET) may be a temporary infrastructure less network, formed by a group of mobile hosts that dynamically establish their own network on the fly without relying on any central administration. Mobile hosts utilized in MANET need to make sure the services that were ensured by the powerful fixed infrastructure in traditional networks, the packet forwarding is one among these services. The resource limitation of nodes utilized in MANET, particularly in energy supply, alongside the multi-hop nature of this network may cause new phenomena which don't exist in traditional networks.*

Keywords: Mobile Ad hoc Network, MANET, Security, Selfish Behavior, Security

I. INTRODUCTON

Traditional wireless network and cellular networks are limited by their need of infrastructure. These networks cover limited geographic area where infrastructure exists only. But sometime we'd like quick network found out with none infrastructure or any access point like within the case of battlefield survivability, communication in disaster areas, communication between vehicles to provide traffic information etc. MANET is that the one solution for these sort of situations. MANET provides multi hop communications by wireless links.

Selfish node is that the critical internal node attack that captures the communication and increases the communication loss. Various researchers have defined different methods for detection and stop selfish node over the network. Selfish attack is one among the sort of denials of service attack. In the network node are going to be act as selfish and doesn't forward the packets of other node towards to save lots of its network resources for own transmission. The node will drop all the packets of other nodes or it may use other mechanisms for saving resources. The proposed technique is uses the watchdog mechanism and therefore the threshold based detection of selfish nodes and prevention of it.

II. METHODOLOGY

MANET represents Mobile adhoc Network additionally called as remote adhoc network or adhoc remote organization that occasionally includes a routable systems administration climate on top of a Link Layer spontaneous organization. They contain set of mobile nodes connected wirelessly during a self-configured, self-healing network without having a hard and fast infrastructure. MANET nodes are liberal to move randomly because the topology changes frequently. Each node behaves as a router as they forward traffic to other specified node within the network.

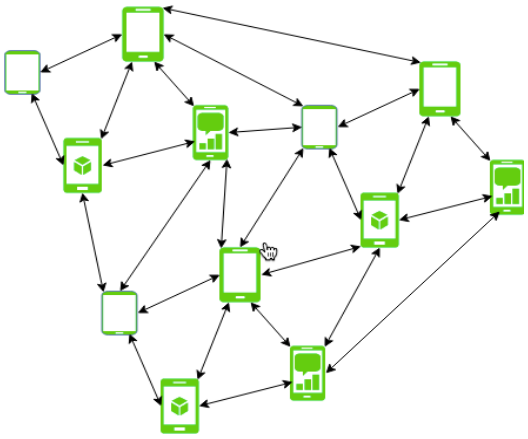


Fig 1: MANET Diagram

Algorithm:
STEP 1:
If a monitoring node hears a neighboring nodes data packet to forward it will check the difference between the last_hTimer and Last_sTimer.

STEP 2:
IF The difference between the timers is within the threshold (last_hTimer - Last_sTimer ≤ threshold)
THEN The node is taken into account as normal and therefore the last service time is updated (Last_sTimer = C_TIME).
ELSE The node is taken into account as suspecious node and further testing is conducted.

STEP 3:
The monitoring node will broadcast a fake RequestREQ packet (with TTL=1 to reduce flooding) and waits for the doubtful node to rebroadcast the Route Re- quest message before time out.

STEP 4:
IF The suspicious node responds before time out

THEN the last service timer (Last_sTimer = CU_TIME) is updated and labeled as normal node.
ELSE The suspicious node is labeled as selfish node (status = selfish).

III. CHALLENGES AND ISSUES

There are a few issues in MANET, for example, the Routing, Multicasting, Transport Control Protocol, etc.

1. **Routing**: Routing protocols are wont to find the optimal path from source to destination node. Routing protocols are used to exchange the routing information. These are vital in MANET where topology changes very frequently thanks to mobility of nodes.
2. **Multicasting**: Multicasting is defined as communication with certain group members during a group. It is a kind of one-to-many communication. Due to characteristics of MANET, the normal wireless network`s protocols aren't suitable for multicasting and hence different protocols are needed which will meet the subsequent challenges for multicasting.
3. **Transport Control Protocol (TCP)**: The main function of the TCP is to provide reliable end-to-end delivery of data packets, flow control and congestion control. Traditional wired control protocol is not used for manet.

IV. ANALYSIS

Here we are providing different methods literature review in detection of selfish nodes to network There are different methods are existing. during this section brief summary of the prevailing methods in detection of manet network is given.

Paper	Used Approaches	Parameters	Remarks
[1]	Attack Tree Algorithm	NA	In This, present differing types of sensors which can be used to find selfish nodes.
[2]	Token Based Method, Agent Based Method, Watch Dog Method	Packet Transmission Ratio, Byte Transmission, Packet Loss, Packet Delay	In this paper, an enquiry to the Selfish node and its working behavior is provided.
[3]	IDS (intrusion detection system)	Throughput, Simulation time	The proposed method not only identifies the attack, it also identifies the range of attack.
[4]	Enhanced Modified AODV	Routing Overhead, Malicious Node Ratio, Avg. End to End delay	In this paper a replacement technique called EMAODV (Enhanced Modified AODV) for preventing and detecting malicious nodes in MANETs is used .
[5]	AODV	NA	In this paper AODV protocol is used for detection and prevention.
[6]	Bays Theorem	NA	In this paper Mathematical Model is used for prevention and detection of selfish nodes.
[7]	IDS (Intrusion Detection System)	Packet Delivery Function, Throughput, End to End delay	In this paper, the proposed IDS scheme work are getting to be excellent to detect and defense the network from selfish node attack.

V. ATTACKS IN MANET

Attacks in MANET can be classified as Active and Passive attacks. An Active attack is one in which an attacker which is a certified node wipe out or alter the data that is being exchanged in the network. While a Passive attack attacker node which is an unauthorized node get the data without disrupting or damaging the network operation.

Another classification can be External and Internal attacks. In External attacks the attacker node is one which do not belong to that network while in Internal attacks the Attacker node belongs to that network. Internal attacks are more severe than External attacks since attacker knows all secret information and have privileged access rights.

a. Black Hole Attack

In this kind of attack, a hateful node participates in route discovery mechanism by sending RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination [11]. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. As soon as the data transmission starts, hateful node drops the data packets that are needed to be forwarded to destinations. Black hole attack is more destructive as compared to gray hole attack.

b. Byzantine Attack

This attack can be done by a single intermediate node or a group of intermediates nodes, behaving as hateful nodes they either create a routing loop or direct the data packets to non- optimal path or selectively drop the packets. Such attacks are difficult to identify.

c. Flooding Attack

In this attack hateful node floods the network with the unnecessary data packets. The victim nodes are not able to receive or forward any data packet and thus any data packet forwarded to such nodes is discarded from the network.

d. Wormhole Attack

In this wormhole attack a hateful node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network [12]. Due to broadcast nature of the radio channel the attacker may create a wormhole for those packets also that does not belong to him.

e. Routing Attacks

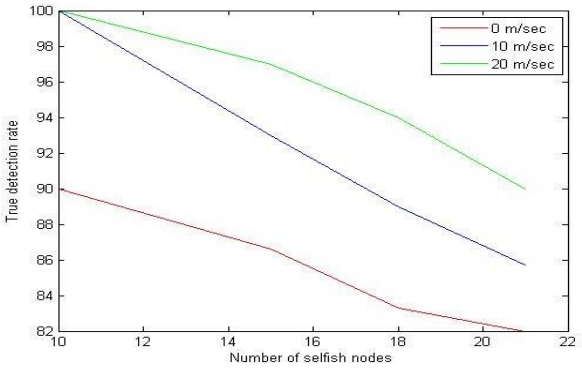
These kinds of attacks affect the normal operation of the routing protocol used in the network. Routing attacks can be of several types in these.

f. Packet Replication Attack

In this attack the hateful node replicates the stale packet and forward to the other node on order to use the battery power and consume bandwidth and create confusion in the routing process.

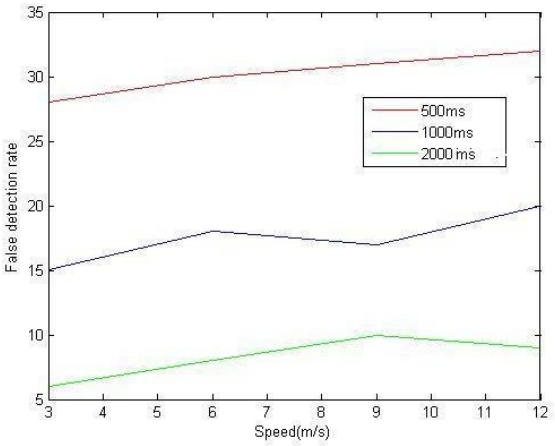
VI. RESULTS AND DISCUSSION

From Figure 2, We notice that when the count of selfish nodes that don't transmit others route request packets are more than the TDR is less this is because when this kind of nodes are more in MANET, then most of the neighbor nodes will be selfish, and the normal nodes which are in the range of these selfish nodes cannot be identified.



Hence, this will lessen the TDR of selfish nodes in

Fig 2



F

ig 3

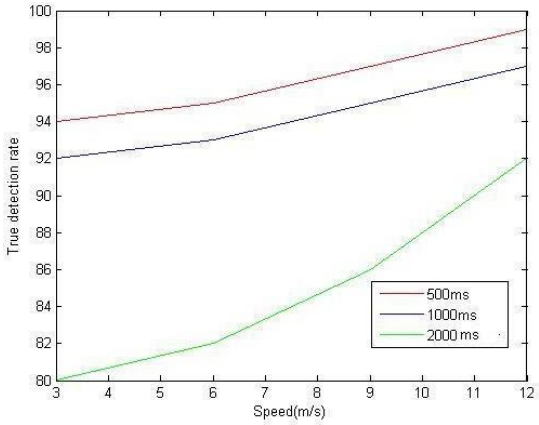


Figure 3: True detection rate of selfish nodes with different moving rates from the Figure 3, we notice the FDR of the selfish nodes is high when the mobility rate of the nodes is high, this is because when a node broadcast a packet to its neighboring node, just in time the neighbor node may go out of communication range and that node will be falsely identified as selfish nodes.

Figure 4: FDR of selfish nodes with different moving rates We also observed the TDR and FDR of selfish nodes with different action hold off times.

From the Figure 4 and Figure 5 we notice that if the

action holds off time is less, the true detection rate is high, this is because if the action holds off time is less than the monitoring of the neighbor nodes will be done more number of times and on the other hand false detection rate increases with the decrease in action hold off time. Lesser the action holds off time worse the false detection rate.

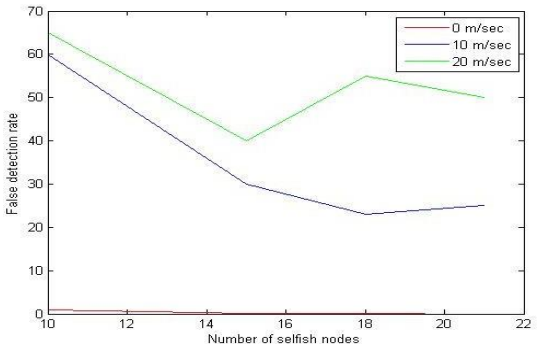


Fig 5

VII. CONCLUSION

We proposed a period based strategy for distinguishing selfish nodes. selfish nodes inside the organization don't offer any types of assistance to other people and save assets to itself. Here we proposed a path for identifying selfish nodes, which don't forward Route Request(RREQ) packets and checked with ns2 simulator, we investigated the false detection rate, recognition rate with various moving rates, distinctive number of selfish nodes inside the organization and with various activity hold off times , we noticed high detection rate when the measure of selfish nodes are less and low action hold off time while false detection rate is a smaller amount when the action hold off time is high.

REFERENCES

[1] Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra,"Security Issues in MANET: A Review",IEEE 2010.

[2] Umang S, Reddy BVR, Hoda MN, "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications 4(17):2084– 2094.2010.

[3] Wu B, Chen J, Wu J, Cardei M, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks" In: Xiao Y,Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York 2007.

[4] Marti S, Giuli TJ, Lai K, Baker M, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August 2000. International Journal of Computer Applications (0975 –8887) Volume 80 – No 14, October 2013

[5] Tseng Y-C, Jiang J-R, Lee J-H, "Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network", Journal of Internet Technology 5(2):123– 130, 2004.

[6] Hu Y-C, Perrig A, Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39, IEEE 2004.

[7] Raja Mahmood RA, Khan AI, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks, International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, November 2007

[8] Mohammed Saeed Alkatheiri, Jianwei Liu, Abdur Rashid Sangi, " AODV Routing Protocol Under Several Routing Attacks in MANETs", 2011 IEEE, 978-1-61284-307-0/11.

[9] Htoo Maung Nyo, Piboonlit Viriyaphol, " Detecting and Eliminating Black Hole in AODV Routing", 2011 IEEE,978-1-4244-6252-0/11

[10] Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks", in Proc. ACM Southeast Regional Conference, pp. 96-97, 2004.

[11] Roopal Lakhwani , Vikram Jain , Anand Motwani , "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.

[12] G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, "Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence", (152-156) Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 978-1-4673-5845-3/

[13] Monika Goyal , Dr. Sandeep Kumar Poonia , Dr. Deepak Goyal, "Attacks Finding and Prevention Techniques in MANET: A Survey", ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1185-1195.