ISSN 2319 - 6629
Volume 8, No.3, April - May 2019
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt02832019.pdf
https://doi.org/10.30534/ijwcnt/2019/02832019

Three-Tier Approach for Identifying Malicious Nodes in MANET

Aifa S[1], Tibin Thomas[2], Nayana Elizabeth Andrews[3]
[1]PG Scholar, Saintgits College of Engineering, India, aifasalih26@gmail.com
[2]Assistant Professor, Saintgits College of Engineering, India, tibin.thomas@saintgits.org
[3]PG Scholar, Saintgits College of Engineering, India, nayanandrews@gmail.com

ABSTRACT

In present days, mobile ad hoc networks have grown into an emerging research topic. One of the challenging problem in MANET is securing it in an unsafe environment. In MANET, Innumerable intermediate nodes interchange information without the need of infrastructure. To cooperate with each node all nodes participate in packet forwarding. Due to the inadequate energy of the nodes they do not participate in the routing process correctly. Existing solutions are not enough to secure the wireless network, as there are many vulnerabilities in using ad-hoc networks. To obtain a tolerable amount of security, conventional security mechanisms should relate to an intrusion detection system. We propose a three-tier approach for identifying malicious nodes in the network. Here, in this paper to identify the nature of the nodes as mischievous or genuine three levels are used. The first level is acknowledgement phase it consists of DTQ function, the DTQ value of nodes will be near to a constant or will be dynamic value for a legitimate node and will be continuously decreasing for a mischievous node. The second level is the voting phase, used to confirm the node is malicious. The third level is credit value phase used to identify the malicious nodes among the voter nodes in level two.

Key words : DTQ function, Mobile Ad hoc Networks, MANETs.

1. INTRODUCTION

MANET comprises of numerous mobile devices with an effective intermediate node for communication. Security is the critical responsibility for the fundamental purpose of MANET. The network suffers from security interventions because of open atmosphere, changing network structure, absence of central authority and cooperative algorithm. Cooperation of nodes is the main security concern in MANET. MANET is composed of a important number of mobile nodes without a established infrastructure. In multi-hop fashion the in between nodes are used for transferring the packets for other nodes [1]. Hence, each node in MANET forward the packets to other nodes acting like a router.

MANETs are deeply exposed to different security interventions due to the distributed and collaborative nature of routing algorithms. Because of portability of nodes network structure in MANET is changing. Network functions are done by the nodes either independently or cooperatively with other nodes. The MANET becomes more powerful when more nodes assists to shift traffic. Consumption of network frequency range, local CPU time, memory and energy and energy are more during detection of routes and forwarding of packets. Due to these reasons nodes try to preserve their resources, and especially their batteries.

One of the challenging problem in MANET is securing it in an unsafe environment. A conspicuous level of security is achieved by the wired network using gateways and routers. Due to the dynamic topology and absence of precise barrier mechanisms like firewall are not sufficient. A malicious node can easily destroy the entire network. External attacks can be controlled by providing security services like authentication and access control, but there needs some mechanism to protect from the internal attacks. All possible attacks cannot be prevented alone using a defending mechanism [2]. Therefore, there should be an effective mechanism that can deal with the malicious nodes to secure ad hoc network. An intrusion detection system should be implemented to secure the network. MANET can be kept from danger by using IDS.

2. LITERATURE SURVEY

[3] Marti, Giuli, Lai and Baker presents two approaches- Watchdog and Pathrater using DSR routing protocol. Misconducting nodes are identified by the watchdog by observing the later node's communication through immoral mode. If the neighbour node is idle for a predefined time, without forwarding the packet, then the failure counter for that node is increased by one. When the failure counter go beyond the threshold value then that node is noted as misconducting.

[4] Mechanisms like auctions and traditional credit system are incorporated to produce an enhanced version of the AODV routing protocol. During the route discovery, most part of the planned technique is achieved. In this protocol, based on minimum cost end- to- end routes are selected. The cost is calculated based on individual nodes offers.

[5] An interruption identification system called Enhanced Adaptive Acknowledgment (EAACK) was proposed to detect selfish nodes. This model consists of three key components, namely, ACK, Secure ACK (S-ACK), and Misbehaviour Report Authentication (MRA). ACK operates as a part of the combination scheme in EAACK, when no network misbehaviour is detected it intends to reduce network overhead. The S-ACK scheme is an enhanced form of the TWOACK scheme. The objective of presenting S-ACK mode is to identify misconducting nodes in the existence of accepting collision or limited transmission power. The main aim of MRA scheme is to verify that whether the missed packet has accepted to the destination node through a different route. To launch the MRA mode, An different path to the terminal node is made by the source node by searching its local knowledge base. If no routes exist, then the source node sends DSR routing request.

[6] A fast model approach is used to lower the detection time. This approach works based on fast diffusion of selfish nodes awareness from different watchdogs [6]. To improvise the discovery of malicious node in the network a distributed global trust is presented here. Along with removing the terrible effect of false positives, false negatives and greedy nodes this method decreases the period and expand the usefulness of distinguishing selfish nodes. In this mechanism, a trust and reputation method is used for the analysis to advance the identification of attacker nodes [6]. The detected greedy node is noted as non-malicious by the watchdog. Combination of these positive reports by different watchdogs leads to the base of this mechanism. Continuous Time Markov Chain is used to model the performance of the collaborative watchdog mechanism.

[7] In reputation based malicious node detection the capability of reputation based Selfishness Prevention Protocols (SPP) is enhanced by evaluating three techniques that correctly detect real selfish nodes, and increases the efficiency of the whole network. The three techniques involve Reset Activity Mode (RAM), Warning mode (WM) and Reset failure mode (RFM). The reputation is registered in the reputation table by the precursor node and it identifies the amount of faults present in the every other known nodes. A heuristic algorithm, is then completed to identify the path that does not contain selfish node. The central objective of these techniques is to diminish the false allegations created due to radio transmission errors and packet collisions in the accusation decisions [7].

[8] Basic trust mechanism is used in Record- and Trust-Based Detection (RTBD) mechanism for identifying greedy nodes. In this paper, based on their behaviour the sincerity of a node is evaluated. In this framework, a global trust state is maintained by every node for all greedy reacting nodes in the network. A trust table is used to maintain a trust state. There are two fields in the trust table namely id of the node and the trusted value. When a new trust certificate arrives the state of the node is renewed. The reply from every nearby node is checked to verify the certificate. The trust state of the doubtful node is made based on the trust certificate in the final trust value [8]. In this method, a effective tool is used for the identification of malicious node behaviours. The neighbour nodes can avoid the participation with the selfish nodes once they are detected.

[9] A Token Based Umpiring Technique (TBUT), In this method a token is needed to participate in the communication. The neighbour node would act as an umpire that provides status and reputation to the node based on its previous behaviour. A additional field next hop is added to the AODV routing protocol, because of that the node can compare the listened packets accurately. Two algorithms are used in this mechanism. The path identification procedure is made in first algorithm and malicious node isolation procedure is done on second algorithm. [9]. New routes can be dynamically discovered by other node in MANET using route discovery. In the promiscuous listening mode, each node overhears the channel [9]. TBUT aims to detect selfish nodes that don't participate in basic functioning of routing.

[10] Neighbour credit value based AODV routing was suggested for enhancing the current standard AODV convention by a credit amount based routing enhancement. Another field named neighbour credit table (NCT)was kept up by every node which refreshes the credit estimation of its neighbour nodes over time. Hence, this was the significant duty of the neighbour credit table. Every single time an information packet is coordinated from a neighbour or dispatched by a neighbour, the credit amount updating is made in the table if the neighbour node is authenticated. [10].

iNCV-AODV was proposed by improving the NCV-AODV by polishing its efficiency [11]. A few presumptions in iNCV-AODV are the node in the system are basically not attacker node and just a portion of the new node that may act like attacker node. In this component nodes, the neighbour credit table is initialized by giving a sample credit value to its known nodes. As the operation continues the credit values of the neighbour nodes will be renewed. Subsequently, the enemies may add advanced nodes to the system, and after that the credit table will be refreshed along with the current node if and only if those nodes work ordinarily [12]. If those nodes act greedy, in their neighbour credit table their credits will not be updated. Accordingly, no neighbour will anticipate sending or transfer any packet along those misconducting nodes .

3. EXISTING SYSTEM

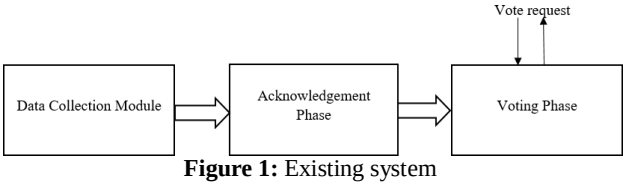

Figure 1: Existing system

Figure 1 shows the structure of the existing system. The system consists mainly of two phases. The first phase is the acknowledgement phase where the data transmission quality(DTQ) value of the collected data is calculated. In this module, the suspected nodes are identified using this data transmission quality value. The second module is the voting module the confirmation of node as malicious is done

in this step. If a node detects a suspected behaviour on other nodes, then they can vote against that node. The misbehaving character is approved by the voting of other nodes. If the number of votes are greater than the threshold value, then it is confirmed as malicious node.

Acknowledgement Phase

In this phase the behaviour of node is identified based on transmission of data. The quality of the node is calculated based on the transmission of data. Based on the acknowledgement received a data transmission quality is calculated. The main duty of the DTQ function is to calculate the communication quality of the nodes. In this phase, each node creates a DTQ table to store the DTQ value of other nodes with which it communicates that is the neighbouring nodes. During the transmission of data to its neighbouring nodes these nodes calculate their corresponding neighbours DTQ value based on the acknowledgement received and store these DTQ value in their DTQ table. The structure of DTQ table consist of a field called time stamp this field shows the time at which last update of DTQ value occurred. If the DTQ value for a node is less than the threshold value, then it is passed to the next phase called voting phase where the decision is taken based on the voting of other nodes based on the DTQ value present on their DTQ table [12].

Voting Phase

Once the voting phase get a request for voting it starts the voting process, that is it broadcast the request to other nodes to vote for the requested node based on the DTQ value present on their DTQ table. Either the node votes for the requested node by sending 1 as a message otherwise it does not vote by sending 0 as a message. The message 1 indicates that the DTQ value of the requested node in its DTQ table have a DTQ value less than the threshold value that the node is suspected. The message 0 indicates that the DTQ value is greater than the threshold value and the node is not suspected. When the request is broadcasted the initiator node keep track on the votes that it receives. A timer is set when the initiator node initialise the request [12]. If the time out occurs, it stops collecting the votes and based on the collected votes it determine whether it is suspicious or not. The main disadvantage in this module is that the voter nodes may be malicious. Therefore, the third phase called credit value phase is introduced to identify the malicious nodes among the voters.

4. PROPOSED SYSTEM

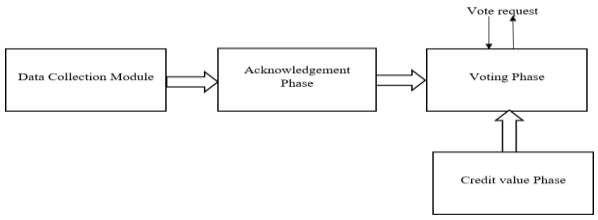

Figure 2: Proposed system

In the existing system, the main disadvantage is that voter node may contain malicious node. To identify malicious node among the voter node a new phase called credit value phase is introduced. The third phase is the credit value phase where the malicious node among the voters are identified based on their credit value as shown in figure 2.

4.1 Credit value phase

This phase is introduced to identify the malicious nodes among the voters in the voting module. A credit value concept is introduced, a credit value table is created for every node the credit values will be incremented based on the communication. Initially a value is given to all nodes and the credit value is increased based on the transmissions made. If a node makes a request and if a node replays with a solution to the request, then the credit value of the replayed node and the requested node will be incremented in their credit tables respectively. As the credit value for a node is higher than it is considered as a non-malicious node because the communication made by it will be more. Therefore, in voting module when the initiator node gets these votes then it will only accept the votes from nodes having a minimum credit value and rejects the votes from the node having credit value less than a threshold value.

5. CONCLUSION

One of the challenging problem in MANET is securing it in an unsafe environment. In MANET, Abundant intermediate nodes interchange information without the need of infrastructure. MANETs are deeply exposed to different security interventions due to the distributed and collaborative nature of routing algorithms. Because of portability of nodes network structure in MANET is changing. In this paper, we proposed a mechanism to identify the malicious nodes among the voter nodes. The malicious node is identified using a credit value. Based on the credit value the votes are accepted, using this method the voting from malicious nodes can be eliminated.

REFERENCES

1. S. Kumar. **Detecting and avoiding selfish nodes in delay tolerant networks(DTNs)**,*International Journal of Recent Research Aspects, vol. 5, pp. 325-329, March 2018*
2. K. Dutta, S. Kumar and G. Sharma. **A detailed survey on selfish node detection techniques for mobile ad-hoc networks,***Fourth international conference on parallel distributed and grid computing, 2016*
3. S. Marti, T. Giuli, K. Lai, and M. Baker.**Mitigating routing misbehavior in mobile ad hoc networks,** *Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, pp.255-265, 2000* https://doi.org/10.1145/345910.345955
4. C. Demir and C. Comaniciu. **An auction based AODV protocol for mobile ad hoc networks with selfish nodes,** *IEEE International Conference, pp. 3351-3356, 2007*

5. E.M. Shakshuki, N. Kang, and T.R. Sheltami. **EAACK—A secure intrusion-detection system for MANETs,** *IEEE transactions on Industrial electronics, vol. 60, No. 3, pp. 1089-1098, 2013*

https://doi.org/10.1109/TIE.2012.2196010

6. E. Hern´andez-Orallo, M.D. Serrat Olmos, J.C. Cano, C. T. Calafate and P. Manzoni. **A fast model for evaluating the detection of selfish node using collaborative approach in MANET's,** *Wireless Personal Communications, vol. 74, no. 3, pp.1099-1116, 2014*

https://doi.org/10.1007/s11277-013-1346-y

7. A. Rodriguez-Mayol and J. Gozalvez**. Reputation based selfishness prevention techniques for mobile ad-hoc networks,***Telecommunication Systems, vol 57, no. 2, pp.181-195, 2014*

https://doi.org/10.1007/s11235-013-9786-y

8. S. Subramaniyan, W. Johnson and K. Subramaniyan. **A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique,***EURASIP Journal on Wireless Communications and Networking, vol. 2014, no. 1, 2014*

https://doi.org/10.1186/1687-1499-2014-205

9. J. Kumar, A. Kathrival, N. Kirubakaran, P. Shivraman and M. Subarmaniam. **A unified approach for detecting and eliminating selfish nodes in MANET's using TBUT,** *EURASIP Journal on wireless communication and networking, vol. 2015, no. 1, pp. 1-11, 2015*

https://doi.org/10.1186/s13638-015-0370-x

10. R. Abirami, K. Sumithra, M.G**. An improved neighbor credit value based AODV routing algorithm for preventing the impact of selfish behaviorunder MANET**, *WorldAppl.Sci.J.35(3),334–343 (2017)*

11. R. Abhirami, K. Sumithra. **Evaluation of neighbour credit value based AODV routing algorithm for selfish node detection,** *Cluster computing, 2018*

https://doi.org/10.1007/s10586-018-1851-6

12. M. A. Selvan, S. Selvakumar**. Malicious node identification using quantitative intrusion detection techniques in MANET**, *Cluster computing, 2018*

https://doi.org/10.1007/s10586-018-2418-2