Trust Based Collaborative Watchdog Technique for Selfish Node Detection in Multi-hop Neighbours

Sheeja M K

Final Year M.Tech Degree, Dept. of Computer Science and Engineering
Cochin Institute of Science and Technology, Muvattupuzha, Kerala, India

Abstract *-A mobile ad hoc network is a wireless network in which no infrastructure is available. MANET is a self-configuring network. Due to dynamic nature of MANET it is very challenging work to employ a secure route. The intermediate nodes cooperate with each other as there is no such base station or access point. The routing protocols play important role in transferring data. Cryptographic mechanisms are used in routing protocols to secure data packets while transmitted in the network. But cryptographic techniques incur a high computational cost and can't identify the nodes with malicious intention. So, employing cryptographic techniques in MANET are quite impractical as MANETs have limited resource and vulnerable to several security attacks. Trust mechanism is used as an alternative to cryptographic technique. Trust mechanism secures data forwarding by isolating nodes with malicious intention using trust value on the nodes.*

The most important aspect of the proposed system is that it is able to identify the selfish nodes or the attackers in the two-hop neighbours also, as opposed to other watchdog techniques which can detect selfish nodes in one-hop neighbours only. The attackers are having a trust value less than the threshold trust value and such nodes are eliminated from the route. If one node finds that one of its one-hop neighbours or two-hop neighbours is an attacker, then the corresponding change is made in the so called trust table so that other nodes will also be aware of the attackers and thereby they can avoid them while selecting the route to send their packets. This helps to achieve a packet drop of zero or a packet delivery ratio of one in all the cases, thus improving the overall efficiency of the network.

Keywords – *MANET, attacker, trust, multi-hop neighbour*

I. INTRODUCTION

A mobile ad hoc network is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use ,and therefore be a router. Each device is considered as a node in a MANET. The primary challenge in building a MANET is equipping each device to continuously maintain information required to properly route traffic. All the nodes have to work in a collaborative manner to provide a better route for the data packets to reach the destination. Just like we have people who behave differently, there are nodes also which behave in a different manner. Some nodes in the network may not be trustworthy. Such nodes are known as selfish nodes or attackers. They attack then smooth functioning of the packet forwarding process, which may lead to increased packet drop or decreased packet delivery ratio. We always aim at a zero as the packet drop value or one as the packet delivery ratio, which means that all the packets which are sent from the source must reach the destination. If this has to be accomplished, then the selfish nodes must not be included in the route from source to destination. The selfish nodes must be completely excluded from the routing path. A collaborative watchdog technique is used to detect the selfish nodes. Since MANETs are running with multi-hop neighbours this paper deals with selfish node detection in multi-hop neighbours, especially two-hop neighbours.

II.RELATED WORKS

[S. Bansal, M. Baker, 2003] If a node observes another node not participating correctly, it reports this observation to other nodes who then take action to avoid being affected and potentially punish the bad node by refusing to forward its traffic. Unfortunately, such second-hand reputation information is subject to false accusations and requires maintaining trust relationships with other nodes.

[S. Senthilkumar, J.William, 2014] In a reputation based technique, each node is responsible for monitoring the transmission of a packet to neighbour node, or obtaining the status of other nodes from a centralized node on the network. If a node successfully contributes in the

transmission of data by forwarding data packets, the reputation of the node is increased, or if the node discards the packet by dropping it, the reputation is decreased. After the nodes reputation drops below a threshold set by the developer, the node is either punished or ignored.

[Mr. Swapnil S. Shinde, Dr. B. D. Phulpagar, 2016] In Watchdog technique, each node has a mechanism which overhears the medium to check whether the next-hop node faithfully forwards the packet or not. Each node maintains buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If it overhears forwarding, removes the packet from the buffer and determined that node as a normal node. If a packet has stayed in the table for longer than a certain period, the module increments a failure count for the node responsible for forwarding on the packet. If the count exceeds a certain threshold value, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

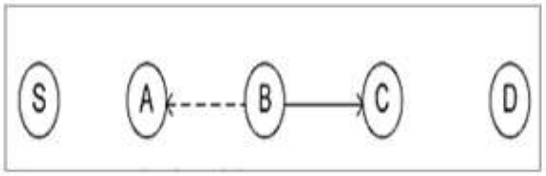

Fig. 1 An illustration of watchdog

"S" is the source node and "D" is the destination node. The other nodes are intermediate nodes in the route between 'S' and 'D'. Before 'A' forwards a packet received from 'S', it saves the packet in its watchdog monitoring buffer. After forwarding the packet to 'B', 'A' monitors whether the packet has been forwarded to 'C'. This is because 'A' is expected to receive a copy of the packet forwarded to 'C' since it's within 'B's transmission range. 'A' then compares the received packet with the one saved in its watchdog monitoring buffer. If 'A' fails to receive a copy of the packet from 'B' within certain duration, it reduces the confidence level of 'B' by 0.05. When this happens in recurring manner, the confidence level is set to zero and 'A' decides that 'B' is a malicious node and sends an alarm so as to change the route through 'B'. Meanwhile if 'B' forwards the packet within the time duration, 'A' rewards 'B' by increasing its confidence level by 0.01.

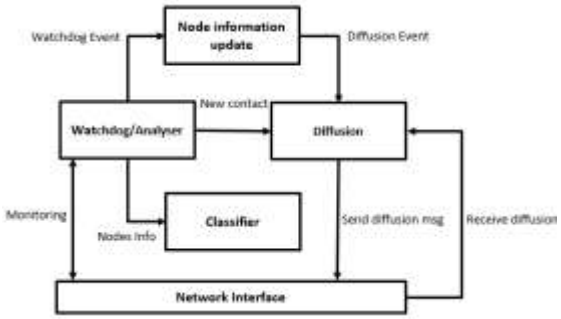

Fig. 2 Architecture of Watchdog System

The Strength of this mechanism is to detect selfish node accurately and to maintain the throughput of the system at an adequate level even with a more number of misbehaving nodes and it can identify selfish node in link layer and network layer.

In the system work which use the local watchdog method to detect the selfish nodes, the watchdog generates positive detection if the node behave s selfishly an d a negative detection if the bode behaves properly as expected. There is selfish node detection and diffusion of information when contact occurs between each pair of neighbours. Every node has a watchdog which will be continuously monitoring the behaviour of other nodes to check whether they are selfish or note. If it finds that a particular node is selfish, then it does a corresponding in formation update in the table to make the information available to all other nodes so that they will not include selfish nodes in their routing paths.

The main drawback of such a system is that it can find the selfish nodes in its adjacent neighbours only or such techniques works with one-hop neighbours only. This paper brings out a solution to this by considering two- hop neighbours also.

III. SIMULATION ENVIRONMENT

NS2.35 is used to simulate the proposed system. Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS can simulate the following:

1. **Topology:** Wired, wireless
2. **Scheduling Algorithms:** RED, Drop Tail,
3. **Transport Protocols:** TCP, UDP
4. **Routing:** Static and dynamic routing

5. Application: FTP, HTTP, Telnet, Traffic generators

NS2 is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed freely and open source. A large amount of institutes and people in development and research use, maintain and develop NS2. This increases the confidence in it. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X.

IV.SIMULATION PROCEDURE

The system detects selfish nodes in one-hop and two-hop neighbours based on the trust value of the nodes.

Trust Value Calculation

Every node in the system is associated with a trust value. This trust value is calculated based on the positive responses it gets from the recipients of the message it sends. For example, if a node sends message to five nodes and it gets three positive responses, then the trust value of that node is 3/5. Similarly every node has a trust value and these values are stored in a table called trust table. The system uses a particular value as then threshold value for this trust and the nodes whose trust value falls below this will be considered as the selfish nodes and they will not be included in the routing path. The trust value of the nodes can be detected by any node in the network. Whenever a node finds that a particular node is not trustworthy, then the trust value of that node is updated in the trust table.

The trust values are not static. A node can become selfish at any point. Therefore, the nodes have to keep track of the trust table to determine the next node in its routing path. A particular node is selected based on its trust value and the distance to the destination. If two nodes are in the list which are trustworthy, then the one which has shorter distance to the destination will be selected.

The concept is to create on each node a trust repository (Trust Table), which will maintain and handle trust information about each neighbouring node. In the Trust Table values regarding a number of events are stored; based on these values, a total trust value is calculated which is then incorporated in the routing function in order to drive the selection of the forwarding node. One of the most important aspects of the trust management schemes is the process of data collection. The direct trust value of a neighbouring node can be determined by its multi-attribute, time-varying trust value depending on a set of events.

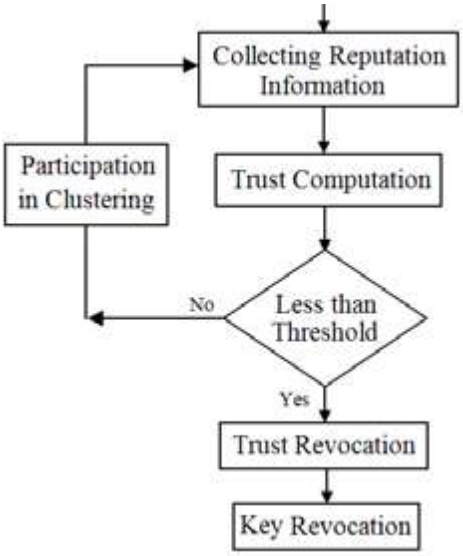

Fig.3 Trust Evaluation Process

V. SIMULATION RESULTS

The system works equally well with one-hop neighbours and two-hop neighbours. For each node, the list of oone-hop neighbours and two-hop neighbours will be stored in a table. One node can identify any selfish node in its two- hop neighbours also. It succeds in achieving a packet delivery ratio of 1 and packet drop ratio of 0 as shown below.

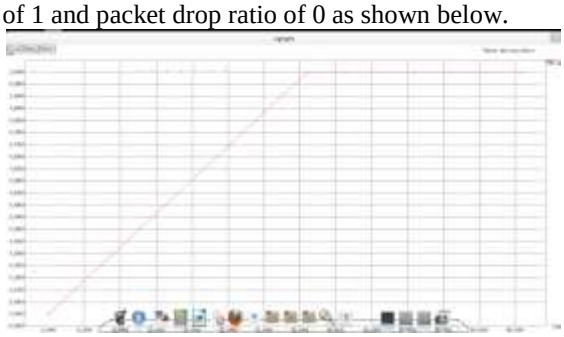

Fig.4 Graph showing packet delivery ratio

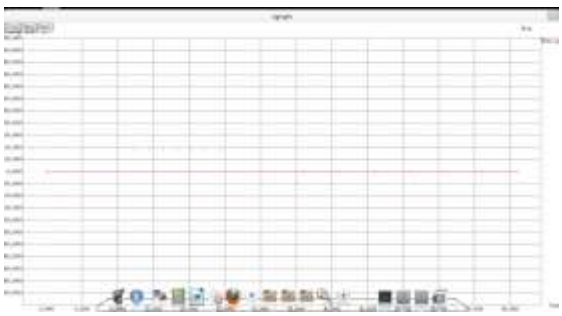

Fig. 5 Graph showing packet drop ratio

IV.CONCLUSION AND FUTURE WORK

Selfish node detection in multi-hop neighbours proves to a boon in the field of communication in Mobile ad Hoc Networks. As a future work, we can fix the trust value to be 1 so that only the most trusted nodes will participate in the routing.

REFERENCES

[1] S. Bansal, M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks" arxiv:cs.ni/0307012, 2003.

[2] M. Hollick, J.Schmitt, C. Seipl, and R. Steinmetz, "on the Effect of Node Misbehaviour in Ad Hoc Networks," in proc. ieee int. conf. commun., 2004, pp. 3759–3763.

[3] S. Senthilkumar, J.William, "a Survey On Reputation based Selfish Node Detection Techniques in Mobile Ad Hoc Network" in Journal Of Theoretical And Applied Information Technology, 20th february 2014. vol. 60 no.2.

[4] Mr. Swapnil S. Shinde, Dr. B. D. Phulpagar, "A Collaborative Watchdog and Classifier based Scheme to Detect and Avoid Selfish Nodes in MANET" in International Journal of Engineering Sciences & Research Technology, February, 2016,pp. 658-664.

[5] Gayathry S S, R N Gaur," Handling Selfishness in MANETs – A Survey" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 11, November 2014.

[6] M.Madhumathi, S. Sindhuja, "A Survey on Collaborative contact-based Selfish node detection in Mobile ad hoc Network" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4 Issue 10, October 2015.

[7] Kennedy Edemacu1, Martin Euku2and Richard Ssekibuule3, "Packet Drop Attack Detection Techniques In Wireless Ad Hoc Networks: A Review" in International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014.