An Efficient Detection Of Selfish Nodes Based On Collaborative Contact Based Method

P.Sathyia
PG Scholar, Dept. of CSE,
V.S.B Engineering College,karur,TN
Sathyamooorthy.sathy75@gmail.com

Mrs.C.Suguna
Assistant Professor, Dept. of CSE,
V.S.B Engineering College, Karur,TN
mcsuguna@gmail.com

Abstract— Network security consists of the policies adopted to prevent and monitor authorized access to data in a network,Which is controlled by the network administrator. Mobile Adhoc network consists of multiple mobile nodes in the network, where the nodes would move in different direction based on which new path would be established. The collaborative network is the one where the multiple nodes may communicate with other to share resources, thus there is no need to get permission for data access. The major limitation of collaborative MANET is presence of selfish nodes which might refuse to transfer the packets to other nodes to save their resources from wastage. In the existing work, collaborative contact based watchdog is proposed which will find the selfish nodes by communicating with every nodes present in the environment. The compromise between the selfish node and monitoring would prevent the detection ratio of selfish node detection. This is overcome in the proposed methodology by introducing the technique called Divergence based Malicious Monitoring Node Detection (DMMND) which attempts to find the malicious monitoring nodes present in collaborative MANNET environment by predicting the divergence present in the usual behavior. The divergence is calculated by using the methodology called the kullback-Leibler divergence (Kl divergence) which could identify the malicious monitoring nodes accurately. The experimental conducted was proved that the proposed methodology can predict the selfish behavior of nodes more accurately than the existing approaches.

Index Terms— Mannets, Selfish nodes, DMMND, Kl divergence

I. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing.

However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs.

Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. A Mobile Ad Hoc Network (MANET) is a continuously self configuring, infrastructure-less network of mobile devices connected without wires. Ad Hoc is Latin & means “for this purpose” Each device in a MANET is free to move independently in any direction and will change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. They may contain one or multiple & different transceivers between nodes.

II. RELATED WORK

Many approaches have been proposed to detect selfish nodes have been proposed. For example, Jim Solomon Raja., et al [1] suggested that analysed a process of finding the malicious nodes present in the mobile Adhoc environment in terms of selfish behaviour. This survey discusses a various techniques which focus on finding the selfish behaviour of the nodes that are present in the environment in terms of their packet forwarding behaviour. Senthil Kumar Subramaniya, et al [2] introduced the novel approach for detecting the selfish nodes present in the distributed environment. This is achieved by maintaining the record and trust based method which will create the table and stores the packet transmission rate. Dipali Koshti., et al [3] suggested that conducted a survey analysis to...
find the better algorithm that is used to find the malicious nodes in the efficient manner. Mechanism and procedures of various protocols has been studied and discussed in the efficient manner. The main protocols that has been compared for which can find the malicious node in the efficient manner are AODV and DSR protocols. Both of these protocols works with the consideration of forward packet transfer behaviour. Hongxun Liu, et al [4] suggested that introduced the novel mechanism for the detecting the malicious behaviour of selfish nodes in the mobile Adhoc environment. This novel mechanism will maintain the hardware cache storage in the each and every nodes present in the environment. The hardware cache will store the every innovative packet that is transferred through the corresponding node. The detection mechanism will compare the original packet with the hardware cache stored packet in information to find the divergence of both packets.

II. SYSTEM DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development blends the perspective of marketing, design, and manufacturing into a single approach to product development.

Existing System

Mobile ad-hoc networks (MANETs) rely on cooperation of all participating nodes. Thus they are vulnerable to selfish nodes using the net without providing own resources, as well as malicious nodes attacking the net infrastructure. With this simple approach a node sends a packet to its neighbour and then overhears the neighbour forwarding it one hop further along the route. Thus a misbehaving node dropping or manipulating packets is immediately identified and routes using this node can be avoided (using a so-called pathrater component to choose the best route). Unfortunately this mechanism is too simple and has two major drawbacks. First: it is error-prone; a packet collision between AB causes a false negative detection (A does not recognize successful retransmission) and a collision between BC causes a false positive detection (A acknowledges the retransmission even though it failed). The model also relies on all clients to have equal sending ranges – this conflicts with modern WiFi controllers using energy control. Second: When a node recognizes its neighbour as non-participating it does not speed this information, but is only supposed to find a new route around the problem, thus even rewarding the non-participating node (now it does not have to forward other node’s data anymore). For the node on its own it is perfectly rational to avoid the selfish node and increase its own throughput – but for the net at large this is a bad choice as it does not punish the selfish node but only burdens the cooperating ones with more work.

Proposed System

Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks. Existing work introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. The goal of this approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.

It is based on the combination of a local watchdog and the diffusion of information when contacts between pairs of nodes occur. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections.
III. SYSTEM IMPLEMENTATION

The occurrence of selfish node present in the network environment which might lead to failure of execution of overall network environment. This problem needs to be considered in the proposed methodology in terms guaranteeing the secured transmission of data packets. It has the followings

Network Model

The network is modelled as a set of N wireless mobile nodes, with C collaborative nodes, M malicious nodes and S selfish nodes (N = C + M + S). Our goal is to obtain the time and overhead that a set of D <= C nodes need to detect the selfish nodes in the network

Cocowa Model

The local watchdog is modelled using three parameters: the probability of detection p_d, the ratio of false positives pf_p, and the ratio of false negatives pf_n. The first parameter, the probability of detection (p_d), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a PosEvt or NegEvt event. This value depends on the effectiveness of the watchdog, the traffic load, and the mobility pattern of nodes. For example, for opportunistic networks or DTNs where the contacts are sporadic and have low duration, this value is lower than for MANETs. Furthermore, the watchdog can generate false positives and false negatives. A false positive is when the watchdog generates a positive detection for a node that is not a selfish node. A false negative is generated when a selfish node is marked as a negative detection. In order to measure the performance of a watchdog, these values can be expressed as a ratio or probability: pf_p is the ratio (or probability) of false positives generated when a node contacts a non-selfish node, and pf_n is the ratio (or probability) of false negatives generated when a node contacts a selfish node. Using the previous parameters we can model the probability of generating local PosEvt and NegEvt events when a contact occurs:

- PosEvt event: the node contacts with the selfish node and the watchdog detects it, with probability p_d (1 - pf_n). Note that a false positive can also be generated with probability p_d . pf_p.

- NegEvt event: the node contacts with a non-selfish node and detect it with probability p_d (1 - pf_p). A false negative can also be generated when it contacts with the selfish node with probability p_d . pf_n.

The diffusion module can generate indirect events when a contact with neighbour nodes occurs. Nevertheless, a contact does not always imply collaboration, so we model this probability of collaboration as pc. The degree of collaboration is a global parameter, and it is used to reflect that either a message with the information about the selfish node is lost, or that a node temporarily does not collaborate (for example, due to a failure or simply because it is switched off). In real networks, full collaboration (pc = 1) is almost impossible.

Attacker Model

Malicious nodes attempt to attack the CoCoWa system by generating wrong information about the nodes. Thus, the attacker model addresses the behaviour or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a selfish node, or a negative about a selfish node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledge about the way CoCoWa works. The effectiveness of this behaviour clearly depends on the rate and precision that malicious nodes can generate wrong information. Malicious nodes are assumed to have communications hardware similar to the rest of nodes, so they can hear all neighbour messages in a similar range than the rest of nodes. Nevertheless, the attacker could use high-gain antennas to increase its communications range and thus disseminate false information in a more effective manner.

Detection of Selfish node

The goal is to obtain the detection time (and overhead) of a selfish node in a network. This model takes into account the effect of false negatives. False positives do not affect the detection time of the selfish node, so pf_p is not introduced in this model. Using λ as the contact rate between nodes, we can model the network using a 4D continuous time Markov chain (4DCTMC). For modelling purposes, the collaborative nodes are divided into two sets: a set with D destination nodes, and a set of E = C - D intermediate nodes.

Evaluating False Positives

We now develop a model for evaluating the effect of false positives. This model evaluates how fast a false positive spreads in the network (the diffusion time). Thus, in this case, a greater diffusion time stands for a lower impact of false positives. The diffusion time is similar to the detection time of true positives described in the previous section, and it can be obtained in a similar way. Following the same process that in the previous model for the false negatives, we have a 4D-CMTC with the same states (d_p, d_n, e_p, e_n), but in this case c_p = d_p + e_p represents the number of nodes with a false positive, and c_n = d_n + e_n the number of nodes with a (true) negative detection. We can derive expressions similar to 4 and 5, for the case of false positives. In this case, R_p represents the rate of a false positive, and it is derived in a similar way:
\[ R_{fp} = \lambda (\delta_{p,fp}p + \max (pc\epsilon(\gamma cn) + M pm,0)) / \theta \]

and \( R_n \) represents the rate of negative detection:

\[ R_n = \lambda (\delta_{n,fp}(1 - P_{fp}) + \max (pc\epsilon(\gamma cn - c_p) - M pm,0)) / \theta \]

Using these expressions, the transition rates (qij) of the generator matrix \( Q \) are similar to expression 3, substituting \( R_P \) and \( R_{fp} \) by \( R_f \) and \( R_n \), respectively. Finally, using Equations (6) and (7) described in our previous model, we can obtain the diffusion time and the overhead.

**Conclusion**

This work proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost). This reduction is very significant, ranging from 20 percent for very low degree of collaboration to 99 percent for higher degrees of collaboration. Regarding the overall precision we show how by selecting a factor for the diffusion of negative detections the harmful impact of both false negatives and false positives is diminished. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively. Additionally, we have shown that CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited.

**ACKNOWLEDGMENT**

Ms. Sathya P, Currently pursuing ME in CSE at VSB Engineering College. Her research interests include Data Mining and Network security, under the guidance of Mrs. C. Suguna.

**REFERENCES**


