Identification of Trusted Nodes in Mobile Adhoc Network

Jeemi Sinha[1], Chaitali Choudhary[2]

[1]Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India

[2]Associate Professor, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India

Abstract: ***Mobile ad hoc network system (MANET), contain a network area with nodes. In a mobile ad hoc network system, each node has to rely on others to relay its data packets. Since most mobile nodes are typically constrained by power and computing resources, so some nodes may choose, not to cooperative by refusing to do so while still using the network to forward their packets. Most previous works focus on data forwarding. However, dropping control packets is a better strategy for the selfish nodes to avoid themselves from being asked to forward data packets and hence could conserve resources for their own use. In this paper, we present a new system to detect those selfish nodes and simulate result using NS2 tool. 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. In this paper we only present the review and propose system for selfish nodes detection using a NS2 tools. Currently we are working with following keyword for practical implementation of this paper.***

Keywords: MANET, Misbehaving nodes, Trusted Nodes, Network Simulator 2, Adhoc network.

1. Introduction

Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. A MANET is a group of wireless nodes that can be established without any infrastructure or centralized administrator. These nodes can act as both host as well router to forward the packet to other nodes. MANETs have some special features such as wireless media (links) used for communication between nodes, dynamic topologies, limited bandwidth, battery lifetime, and computation power of nodes etc. For the flexibility of MANETs, these characteristics are essential. The inherent features of mobile ad hoc networks make them more vulnerable to a wide variety of attacks by misbehaving nodes. Cryptographic primitives like key distribution and authentication are usual mechanisms used for implementing security in MANETS. But these schemes cannot be used for providing security against such attacks like packet dropping by misbehaving nodes. Node misbehaviour is the behaviour that acts against the cooperative requirements of MANET. A misbehaviour threat can be defined as an unauthorized behaviour of an internal node that can result unintentionally in damage to other nodes, i.e., the aim of the node is not to launch an attack, but it may have other aims such as obtaining an unfair advantage compared with the other nodes [1]. Various distinct dimensions of misbehaviour are: Malicious nodes and selfish nodes. The nodes belonging to first category are either faulty and thereby cannot follow a protocol or are intentionally malicious that try to attack the system. A selfish node on the other hand is a node whose objective is to maximize its own welfare. Since forwarding a packet will incur a cost, a selfish node will get benefit of doing so [2]. Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. There are different motives that insist some nodes to drop a packet rather than sending the packet to the next node in the route. A packet can be dropped at either MAC or Network layer due to the various reasons like:

- Limited buffer size at MAC layer; hence whenever the buffer is full a new packet coming from higher layers will be dropped.
- At the time of transmission A data packet may be dropped or lost if it is corrupted due to radio transmissions such as interference, hidden nodes and high bit error rate[3]
- A selfish node may deny forwarding a packet to save its resources. So this all misbehaviours are done by some node hence it is very impotent to detect that nodes and prevent them to harm the various network operations. In this paper we propose a cooperative approach that detects and removes the misbehaving nodes from the network and also it gives chance to renter the node which was wrongly detected.

2. Related Work

In this section, we discuss some related work for nodes cooperation in MANETS which is currently a very active and demanding research area. The solutions to the problem falls into two categories: Based on Prevention methods and based on detection and removal methods. In the Prevention Based approach nodes are motivated to we discuss some related work for nodes cooperation in MANETS which is currently a very active and demanding research area. The solutions to the problem falls into two categories: Based on Prevention methods and based on detection and removal methods.

In the Prevention Based approach nodes are motivated to cooperate or preventive measures are carried out so that packets should not be dropped before sending them. In Buttyan and Hubaux proposed a preventive approach, which stimulates nodes to cooperate. They use a tamper resistant hardware module called security module, in each node the main idea of this technique is that nodes which use a service must pay for it to nodes that provide the service. Another preventive mechanism is based on economic game theory approach. In this a distributed and scalable acceptance algorithm called Generous TIT-FOR-TAT (GTFT) based on

NASH equilibrium to stimulate cooperation. The acceptance algorithm is used by the nodes to decide whether to accept or reject a relay request. Detection based solutions detect the misbehaviour in the system at the time of packet forwarding. Many researchers have proposed different solutions. Marti, Giuli, Lai and Baker have proposed the solution to the problem of node misbehaviour in data forwarding in MANETs.

To mitigate the degradation of network throughput due to misbehaving nodes, they proposed WATCHDOG that identifies misbehaving nodes and a PATH RATER component that helps routing protocols to avoid these nodes. PCORE is a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks that proposed security scheme (CORE), in which node co-operation is stimulated by a collaborative monitoring technique and a reputation mechanism.

A collaborative reputation mechanism has been proposed by that calculate the combined reputation value by regarding nodes as requesters and providers and then comparing the obtained results with the original results. In S.Usha, Dr.S.Radha has proposed a cooperative approach to detect misbehaving nodes using a multi-hop acknowledgment scheme which uses N-ack scheme. The Nack scheme requires an end to end Ack packet to be sent between the source and the destination. The destination on receipt of the data packets sent by the source, responds with a Nack packet. The data packet and the Nack packet keep track of the route they travel. Our proposed approach is also a detection based nodes cooperation technique. Several systems have been proposed to detect misbehaving nodes in mobile ad hoc network. This system can be classified into three categories:

A. Credit-Based System

Credit based systems are designed to provide incentives for forwarding packets in the form of virtual money (specifically called as Credit). Nodes earn Credit by providing forwarding services to others and have to pay to get services from other nodes. However, to protect the Credit value from attacks and modification, some costly security modules independent of nodes have to be used. In addition, colluding nodes can agree to forward their own flows to accumulate credits while dropping all other flows. Moreover, a well-behaved node that is not asked to route enough packets could not earn credits and will be unable to send its own packet.

B. Reputation Based System

Reputation-based systems on the other hand rely on building a reputation metric for each node according to its behavioural pattern. A monitoring method used by most systems in this category is called a watchdog. Watchdog was proposed by Marti et al.[10] to detect data packet non forwarding by overhearing the transmission of the next node. Use similar monitoring scheme but then propagate collected information to nearby nodes and are susceptible to false praise and false accusation attacks. Mr. Bansal and Mr. Baker proposed a system called OCEAN [14] where the reputation of a neighbour is evaluated using only locally available information and thus avoid sophisticated and potentially vulnerable techniques of reputation propagation throughout the network. It is reported that even with direct observations of the neighbour; OCEAN performs almost as well and sometimes even better compared to schemes that share second-hand reputation information.

C. Acknowledgement-Based System

The last category is acknowledgment-based systems which rely on the reception of an acknowledgment to verify that a packet has been forwarded. Liu et al[15]. proposed the ACK system where nodes explicitly send acknowledgment two hops upstream to verify cooperation. This system is susceptible to collusion of two or more consecutive nodes. Furthermore, colluding nodes can frame honest ones by claiming not to receive the acknowledgment. All of the mechanisms mentioned above are designed to detect and handle misleading nodes. There are a few systems that have been proposed to detect selfish nodes in a MANET. One example is Context Aware Scheme [16] introduced by Mr. Paul and Mr. Westhoff. This system uses un-keyed hash chains and a promiscuous mode to detect the misbehaviour during route discovery phase. The observers of misbehaviour independently communicate their accusation to the source. To convict a culprit, more than three accusations are needed. If there is only one accusing node, the accusing node itself will be considered to be an attacker. The drawback of this system is that it is more beneficial for a node not to send the alarm message to avoid the risk being the only accuser and regarded as attacker. In, [17] Djenouriet all propose two different techniques to detect two different types of control packet droppers. They suggest the use of two-hop ACK approach for monitoring directed packets (RREP, RRER) and promiscuous-based overhearing technique for monitoring broadcast packets (RREQ).[18]Huanget suggest that the monitoring node simply compares the ratio of relay RREQ number between its neighbour and itself. If the ratio is smaller than a threshold, the neighbour is regarded as selfish and its packet is dropped as the punishment.

3. Methodology

All other and above discussed routing protocols designed for MANET naively assume that all the nodes in the network are cooperative in performing the networking tasks like the DSR. This can be guaranteed if all of the nodes belong to a single authority where all of them have the same common objective. However, that is not the case such as in civilian applications, some of the nodes may behave selfishly and only act towards those that add to their own benefits. Providing network services such as forwarding packets and detecting routes consumes network bandwidth, local CPU time, memory and battery power which are limited in MANET nodes [5]. For example, simulation studies by Buttyan and Hubaux when the average numbers of hops from a source to a destination is around 5, then almost 80% of the transmission energy will be devoted to packet forwarding. By denying services for others, a node could reserve its resources for its own use and stay longer in the network. So there is a strong motivation for the nodes not to cooperate and misbehaving. In general, there are two types of node misbehaving:

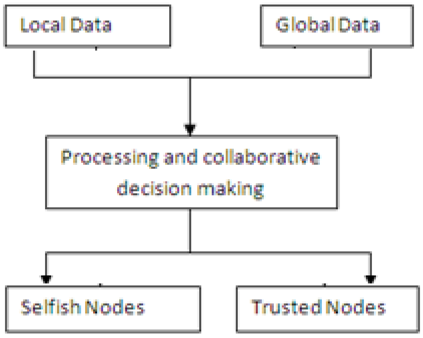
a. Misleading

A misleading node is selective in choosing which packet it wants to respond. It behaves like an honest node, responding to all control packets during route discovery process. However when the node receives a data packet to be further forwarded, the misleading node silently drops it. The reasons for choosing data packets for dropping is because data packets are generally greater in term of size and number than the control packets and thus consumes more energy to forward. This type of behaviour is also called “Gray Hole Attack” [7].

b. Selfish

Selfish node aims to save its resources to the maximum. This type of misbehaving node discards all incoming packets (control and data) except those which are destined to it. By dropping control packets, the nodes would not be included in the routing and then be released from being requested to forward data packets. The similarity of these two types of misbehaving is that they both use the network to forward their own packets but refuse to provide the same services back. Misbehaving nodes can significantly degrade the performance of a MANET. Simulation done by Babakkhouya et al[8] shows that the percentage of misleading nodes can decrease the number of packets that are successfully delivered in the network. When 50% of the nodes of the network become misleading, the packet delivery ratio (PDR) degrades by 55%. Selfish nodes on the other hand, have no big impact on PDR. However, this type of misbehaving can increase the average end to end delay. As the number of selfish nodes been increased, the source node will have less option on which route the data packets should travel. As a result, less attractive route will be selected which means longer delays. It also means that the remaining cooperative nodes have to take the extra burden of forwarding packets. If 50% of the nodes become selfish, the average end to end delay increases by 60%. In this paper, we present a system to detect selfish nodes in a MANET.

System Architecture



The proposed system contains the three modules i.e. Data Gathering and Processing Module, Collaborative Decision Making Module, and Response Operation Module. Every node of MANET contains these modules. The Data Gathering and Processing Module of the system collect data in two ways; first it locally runs a monitoring process to get the behaviour information of neighbour nodes and secondly it exchanges this information with other nodes monitored information. This module then processes the collected information and generates a rate value for every node. The rate value for a particular node is nothing but the behaviour of the node observed by the other nodes in the network. By having the knowledge of rate value the nodes are categorized to the cooperative and non cooperative in the Collaborative Decision Making Module. Finally the Response Operation module performs action according to the decision given by the decision module. In outing operation the misbehaving nodes are ignored.

1. Data Gathering and Processing Module

This module is responsible for collecting nodes behaviour information. It operates in two parts: local information gathering and global information gathering. It stores the collected local and global information in two distinct tables and then process the collected information into the table; Global_rate table to store global information and Local_rate table to store local information. These tables contain one distinct entry for each node. These entry comprises of two information of the node i.e. node id (IP address) and rate value (integer value) fields. The rate value for a particular node defines its observed behaviour.

a. Gathering Local Information

Locally a monitoring process is run in each node for getting information of the behaviour of neighbouring node’. We use new Modified main WATCHDOG that we call as WATCHDOGN, as a monitoring process in our system. All the information monitored here is kept in Local_ rate table. Marti et all proposed the main WATCHDOG technique for monitoring misbehaviour in neighbourhood. It detects misbehaving nodes that do not forward packets. Only negative behaviour of a node is considered in WATCHDOG approach but here. In WATCHDOG-N, a monitoring module always runs in every node for getting the misbehaving of neighbouring node i.e. the nodes which do not forward packet or drop packet. Here we are considering both positive as well as negative behaviour of a node for calculating its rate value. While in Marti et al. WATCHDOG approach only negative behaviour of a node is considered.

The monitor module of each node passively listens to the communication to and from each of its neighbours. For detecting packet drops and modifications by the neighbouring nodes, the monitor module of a node randomly copies the incoming packets to its neighbours and checks whether the neighbours really forward the packets with contents unchanged, or drop them, or modify the contents before forwarding them. The collected data is audited by the monitor. The deviation from normal behaviour of a neighbour is used as an indicator for the unbiased degree of maliciousness; the method of detecting behaviour of nodes is same in both. Lists of recently forwarded packets are maintained in a buffer of each node. Then they are compared with overheard packets by that node for verification. If match is there then the packet is deleted from the buffer and forgotten as it has been forwarded by the next hop node. Here the reputation value of the forwarding node is increased by decreasing its rate value in the Local_rate table. If the packet remains in the buffer for longer than a certain timeout period, that node increases the rate value for the node responsible for forwarding that packet. If the rate value exceeds a certain threshold value, it determines that the node is misbehaving.

b. Gathering Global Information

Every node sends its monitored information Local_rate to all its neighbours, and receives the same from its neighbours observed by them. This received information is kept in a different table Global _rate.

2) Collaborative Decision Making Module
This module is used as a data processing unit. All the collected information is processed here and finally stored in a table Effective_rate. Effective_rate table is then used for routing decisions.
Eff _ ratenew[m] = (Eff _ rate old [m] +global_rate[m] +Local_rate [])/V
Where
V is a variable whose value depends on Global_rate and Local_rate values.

3) The Response Operation Module

In this Module the misbehaving nodes are excluded from the routes on the basis of the behaviour information collected, observed and processed. Node A has been observed to be misbehaving. Source node S wants to communicate to destination need D. As there may be a path from S to D via A but A is excluded due to found misbehaving. Hence Route is established as Sp- q-r-D.

- Local readings are monitored and then forwarded to the neighbours.
- Reputation Value for each node is calculated.
- Decision is made for avoidance of node from the network or to include the node in the network.
- No node immediately declares its neighbour as selfish one but it monitor for a period of time.
- If it exceed from threshold value then only it is treated as misbehaving and hence get avoided...
- In Rating system +ve value define the –ve behaviour of the system while -ve value show the +ve behaviour.
- If false detection comes, it is also solved and the node is reintroduced in the system.

4. Result

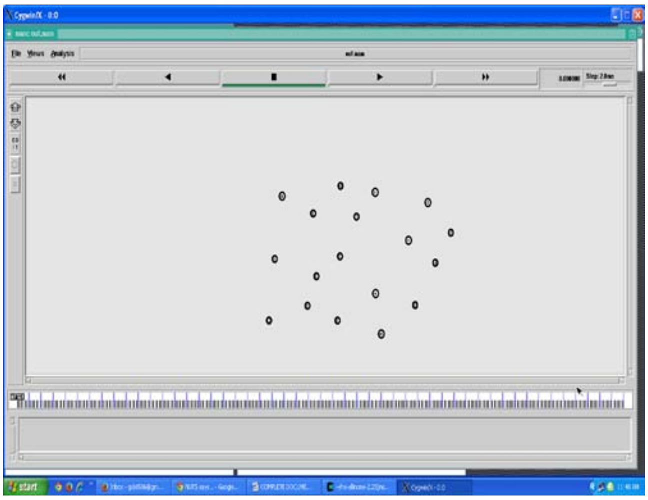
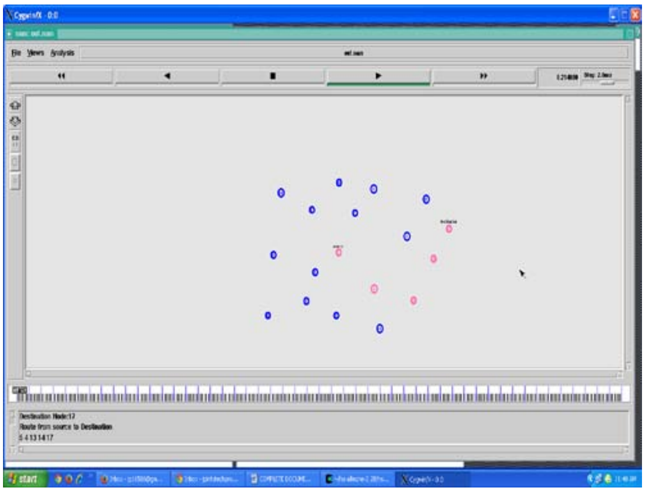
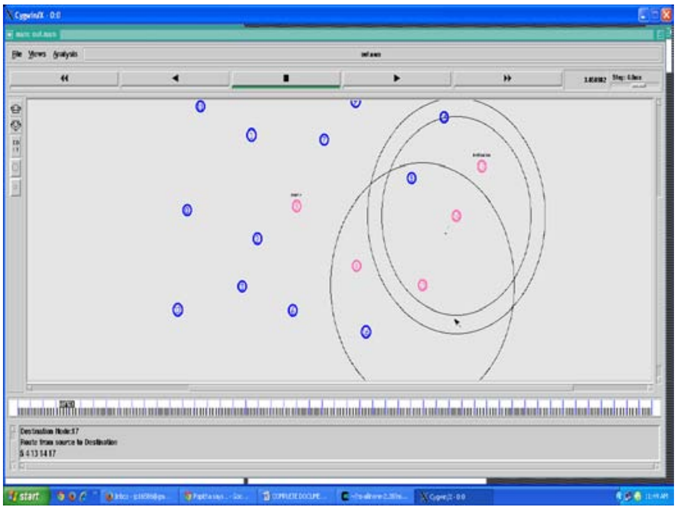


Figure 1: Finding routes in the network



Destination Node:17
Route from source to Destination
5 4 13 14 17

Figure 2: Malicious node identified



Destination Node:17
Route from source to Destination
5 4 13 14 17

Figure 3: Maliicious node not participating in delivering packet

5. Conclusion

In this paper we describe the node's misbehaviour in mobile ad hoc networks and then we have evaluated the effect in network in terms of throughput, overhead, and end-to-end delay. We have proposed a distributed and cooperative approach for improving the Performance of the network by detecting and avoiding the misbehaving MANET nodes. For Simulation, NS2 is used. We get improvement in throughput and very low ratio of false detection of misbehaving node, but at the same time it increases the end-to-end delay as well as overhead transmission. The proposed approach also permits a node which has been false detected to re enter into the network by both negative and positive rating system in which node’s reputation can be gradually improved.

References

[1] Peter Smyth, Mobile and wireless communications: key technologies and future applications (London, UK: IEE, 2004).

[2] Jaydip sen, Piyali Roy Chowdhary, Indrani Sengupta “A Distributed Trust Mechanism for Mobile Adhoc Networks”(IEEE 2006).

[3] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang “Mitigating Packet Dropping Problem In Mobile Ad Hoc Networks: Proposals And Chellenges” 2010-IEEE COMMUNICATIONS SUVEYS & TUTORIALS.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks”, ACM Mobile Computing and Networking, MOBICOM 2000, pp. 255–65.

[5] P. Michiardi and R. Molva., “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks”. In Communication and Multimedia Security 2002 Conference, Portoroz, Slovenia, September 2002

[6] S.Usha, Dr.S.Radha”Co operative approach to detect misbehaving nodes in MANETs using Multi-Hop acknowledgement scheme” IEEE Nov. 2009 International Conference on Advances in Computing, Control and Telecommunication Technologies.

[7] Deb, S. Agrawal, A. Pratab, T. Meyarivan, “A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II,” KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[8] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site)