ISSN: 234-5197
Impact Factor: 2.715

INTERNATIONAL JOURNALOF RESEARCH SCIENCE & MANAGEMENT

AN ENHANCED CROSS LAYER SCHEME FOR BACK OFF ATTACK AND NETWORK LAYER MISBEHAVIOR DETECTION IN MANET

R. Kumaran*[1]& K P K Devan[2]
Department of Computer Science and Engineering, Easwari engineering college

Keywords: Mobile Ad-Hoc Networks, Denial-of-Service, Route Request, Route Reply

Abstract
Mobile Ad-Hoc Networks (MANETs) consist of collection of mobile devices with wireless interface. In MANET, each mobile device acts as both router and host. Nodes agree to forward packets, but fail to do because they want to save their resources. They just keep receiving the data destined to them, and drop the data of other nodes without forwarding or routing them, which reduces the throughput of the network. These nodes are called as misbehaving nodes. Misbehaving nodes deviating from the standard MAC (Medium Access Control) protocol can significantly degrade normal nodes performance and are usually difficult to detect. There are very few techniques to detect and isolate the misbehaving nodes using cross-layer detection schemes. In this work, the main aim is to investigate the cross-layer based schemes to reduce the number of false positive rates and to solve the back off misbehavior in MAC layer. This work also aims to propose an optimized cross-layer based detection scheme.

Introduction
MANET is an autonomous collection of mobile nodes that communicate over fairly bandwidth constrained wireless links. Each node within same transmission range can communicate with each other. Here, nodes can add or leave the network at any point of time. Since the nodes are mobile, the

network topology will change rapidly and unpredictably over time. MANET is composed of mobile nodes without any pre-existent infrastructure and can be placed without any base station and dedicated routers. This property of MANETs enables it to be used in situations where it is costly to deploy an infrastructure such as casual meetings, rescue operations, disaster relief areas etc.
In MANETs, nodes act as both routers and end users. Because of the dynamicity in its environment, routing the packets consistently to the destination becomes a critical issue. In MANETs, packet forwarding requires the co-operation of the intermediate nodes since the packets send from a source has to be relayed via the intermediate node to the destination. Most of the routing protocols assume that the intermediate nodes will relay the packets. The nature of the MANET make co-operation among nodes necessary for the system to be operational. There are two types of MANETs open and closed. In a closed MANET, all nodes will have a common goal and work towards that goal. In

an open MANET, dissimilar nodes have different objectives. Data transmission is the most expensive function in the MANET compared to other functions. Due to the inhibition in resources such as channel bandwidth, Power, CPU, etc, some nodes may refuse to forward or drop the packets which are not destined to them. By misbehaving like this, nodes can save their resources.

1. Misbehaving Nodes In Manet
Node misbehavior can be defined as any form of neglecting the protocol specification to obtain the given goal at the expense of honest participants. A node may misbehave in order to save their resources like (process time and energy). A misbehaving node continues to perform any type of misbehavior till it gain sufficient benefits. Fig 1 shows the packet forwarding in a network with regular nodes and in the presence of misbehaving nodes.

ISSN: 234-5197
Impact Factor: 2.715

INTERNATIONAL JOURNALOF RESEARCH SCIENCE & MANAGEMENT

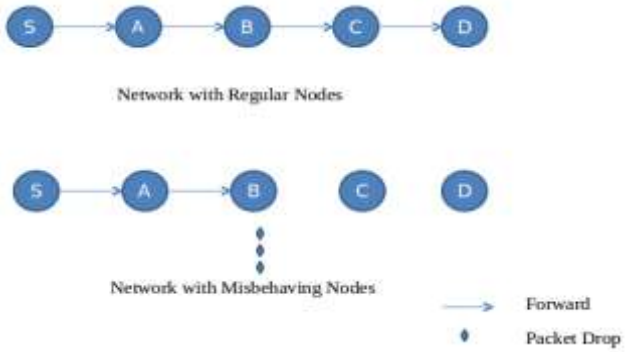

Fig 1 Network with regular nodes Vs misbehaving nodes

Misbehaving nodes can be classified as selfish nodes and malicious nodes. Selfish nodes are those nodes which misbehave to save their energy or power whereas malicious nodes disturb the network operations by its malicious activities. These nodes may take part in the route discovery and route maintenance phases and transmit control packets which can benefit it. However they not grant to forward data packets. Malicious nodes, on the other hand, will participate actively in both route discovery and maintenance phases and transmit the control packets since they need a path to send the data packets so that they can alter or drop those packets.

2. Classification Of Nodes Misbehavior

A normal node is a node who obeys the rules determined by each protocol of its protocol stack. Misbehavior of a node can be defined as purposeful (to save power and processing time) violation of rules specified by a protocol stack. Misbehavior can be categorized based on the violation with respect to a layer. The following layers are considered for the analysis.

MAC Layer Based Misbehavior

In order to access the shared medium, wireless LAN nodes commonly use IEEE 802.11 MAC (CSMA/CA) protocol. Its design attempts to ensure a relatively fair access to the medium for all participants of the protocol. In order to avoid collisions, the nodes follow a binary exponential back-off scheme that favors protocol described for wireless LAN nodes. A node with a packet to transmit selects a random back-off value b uniformly from the set (0, 1,….., W-1), where W is the (fixed) size of the contention window. The back-off counter decreases by one at each time slot that is observed to be idle and the node transmits after b idle slots. In case the last winner amongst the contending nodes. CSMA/CA is a random

access channel is perceived to be busy in one slot, the back-off counter stops momentarily. After the back-off counter is reduced to zero, the transmitter can reserve the channel for the duration of data transfer. The following are the possible violations in MAC layer. Back off attack: Misbehaving node selects the back off value from the range [0, CW/4] instead of [0, CW]. Such misbehaving node disobeys the protocol to gain extra bandwidth at the cost of the neighbor nodes. As a result of this type of misbehavior, such nodes can access the channel (busy state) rather than well-behaved nodes. Fig 2 depicts the back off attack scenario in a network.

ISSN: 234-5197
Impact Factor: 2.715

INTERNATIONAL JOURNALOF RESEARCH SCIENCE & MANAGEMENT

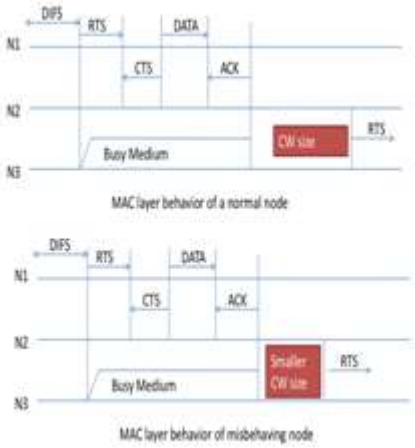

Fig 2 Back off Attack

Network Layer Based Misbehavior

In MANETs, packet forwarding needs the cooperation of the intermediate nodes since the packets send from a source node has to be relayed via the intermediate node to the destination. In Ad-Hoc networks, there are no dedicated nodes that are responsible for forwarding and routing the packets. Hence each node expects the following services from its neighbors: Routing service: This requires nodes to generate route table by the exchange of Route Request Packets (RREQ). Forwarding service: Based on the destination IP address, forwards the packets to the next hop on its path to the destination by referring the route table.

In the Ad-Hoc scenario, following are the possible violations in network layer. Nodes participate in routing process but not in data forwarding process: Misbehaving nodes act well in the route discovery phase and route maintenance phase but refuse to forward the data packets.

In MANETs, RREQ packet size is small. Any node can offer the power for forwarding the packets but data packets are very large packets. Individual dropping: Nodes may drop all or certain percentage of data packets. Colluded dropping: Two misbehaving nodes collude in the network such that the misbehavior of one node will not be reported by the other node. As shown in Figure 1.3, even if node 'A' notes node 'B' dropping the packet, it won't let 'S' know that 'B' is misbehaving. Node 'S' receives a false report from node 'A' as node 'B' which is a well-behaved node So 'A' and 'B' are colluding misbehaving nodes. Fig 3 depicts the Colluding node scenario in a network.

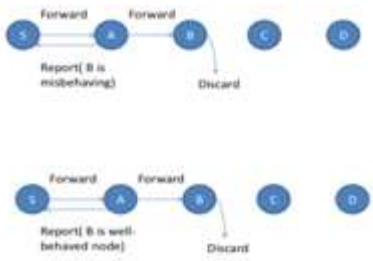

Fig 3 Colluding Nodes

Nodes that do not engage in routing: Some misbehaving nodes do not forward control packets itself. In MANETs, the node is not ready to participate in the forwarding process even for small size packets or in critical state. The transmission path will not be initiated and hence these nodes need not participate in the data transmission.

Related work

In Intrusion Prevention System (IPS) scheme helps to, each monitoring node operates in promiscuous mode and would monitor both data and control packets that are send around within its receiving range. Each monitoring node will keep a record for each of its neighboring node. Through this it can their detect selfish node easily and efficiently, also it decrease the false detection rate up to some extent furthermore it will be suitable for to observe the detection rate and the false detection rate at different moving rate of the nodes. Also plan to investigate the effect of data packet rate to our detection mechanism. A new game theoretic scheme has been proposed for selfish node detection in MANET. This is based on modified AODV routing protocol. data packets will be sent from source node to destination node by computing Least Total Cost Factor (LTCF) . Using payoff matrix we can show that a node will be benefitted if and only if it is cooperative in nature. Otherwise, after a prefix threshold limit is crossed the misbehaving or selfish node will be removed from the network. So, by using this scheme data packets are sent at a lower cost. It also guarantees minimum amount of idle time and promotes cooperation in MANET. Collaborative contact-based watchdog mechanism is a passive acknowledgement based scheme. Watchdog scheme makes use of overhearing mechanism to monitor the neighboring nodes whether they have forwarded the packets or not. They find out the best route by avoiding the misbehaving nodes in the path. It uses an alternate path for further packet forwarding, the misbehaving nodes in the path stay as such. Hence it continues to utilize the network services. In the presence of ambiguous collision this scheme fails to work. In ERCRM (Exponential Reliability Coefficient based reputation Mechanism), a group of mobile nodes having a unique identity are connected in an Ad-Hoc environment which is considered as an undirected graph G = (N, P) where N is a set of mobile nodes and P is the set of paths between mobile nodes. In order to accomplish the objective of detecting and seperating selfish mobile nodes, the following key points are considered. Initially, the amount of energy possessed by each and every mobile node is quantified as evaluated energy metric of that node for detecting Type I and Type III selfish nodes. Secondly, the packet delivery rate of each and every mobile node is manipulated in terms of Exponential Reliability Coefficient through exponential allocation for reconfirming the detection of Type I selfish nodes. Thirdly, Type III selfish nodes are isolated when the estimated energy can drop below the energy threshold value that necessary for a mobile node to exist in cooperative mode. Finally, the isolation of Type I selfish nodes from the active routing path is executed based on the analysis of energy metric and exponential reliability coefficient for enabling reliable data dissemination. Further, ERCRM is a distributed mechanism for reducing selfish nodes in which the reliability coefficient is calculated in each and every mobile node rather than a centralized node. This distributed ERCRM mechanism certainly increases the overhead as (i.e., computation time, bandwidth) and also Average improvement in the packet delivery ratio and throughput by 14%and 17% respectively. An incentive based scheme to detect the selfish node and remove the selfishness is proposed. The scheme reduces dropped rate, message delay, overhead ratio and increase the delivered rate. But on the other hand delivered packets are decreased to increase the selfish degree. In future, it is intended to continue working on it and improve it with the help of formation of the clustering. Next step will be to propose more efficient policies for distribution of credits to participating nodes.

Existing work

The key issues in the existing system can be summarized as follows, In Mac layer, detection scheme is implemented to find the misbehaving node in the network. Previous detection schemes interpreted and implemented the whole network as a hierarchy of layers that are independent and non-cooperating

Proposed system

In proposed scheme, the extend work is "combined solution for routing and MAC layer misbehavior" and combine two schemes to simultaneously check for the nodes misbehavior. The two schemes used here are:

1) Detection scheme for back off misbehavior

Design a distributed back off misbehavior where each monitoring node is continuously monitoring its neighbor node and the observations will be given to decision engine to classify its neighbor node as either normal node or misbehavior node. The proposed detection scheme for back off misbehavior has two stages: observation and decision theory. Node is continuously monitoring their neighboring nodes (observe the number of packets transmitted by the neighbor node) and take sample for each 10 sec. Based on the observation, the monitoring

node checks the value of transmitted packets for their neighbors with their total number of packets received divided by number of neighbors. Then the misbehaving percentage is calculated for each misbehavior node. In this stage, the misbehaving percentage is taken as belief of a node. Then, each node will send a enquiry message to its neighbors and find the other monitoring node with common neighbors. We use Dempster Shafer's Theory of Evidence for bringing out the confident level of identifying misbehaving node. Based on this theory, we combine two belief values and find the node is misbehavior or not.

2) Detection scheme for packet dropping misbehavior

In our proposed technique, by dynamically calculating the nodes forward count values, the source node can be able to find the misbehavior node in the network. Our protocol marks and isolates the misbehaving nodes from participating in the network. So the potential damage caused by the misbehaving nodes is reduced. We make changes to the AODV routing protocol. An additional data structure called Forward Counter Table is maintained by each node.

Misbehavior Detection and Control

Node misbehavior can have adverse effect on network throughput and performance. The following points summarize the degradation of network performance in the presence of misbehaving nodes: A node which uses small contention window will capture the channel without any interruption and give less chance for other nodes to transmit. Packet dropping by any intermediate node assists to degradation of end-to-end performance. Dropping of control packet (RREQ/RREP) leads to unavailability of path in between source and destination or leads to choose longer path between source and destination.

So it is essential to control the negative effects of misbehaving nodes in order to achieve an increase in the network throughput. Detection and controlling are the two phases of misbehavior control. The purpose of detection is to isolate the misbehavior node from the network or to instruct the misbehavior node through punishment. In the decision making module, based on the information accumulated from others and collected by their own, the nodes will make appropriate decisions about other nodes.

i. Detection

The function of the detection phase is to recognize the misbehaving nodes in the network. For each type of misbehavior, decision rule set is defined for all nodes inside the network. The estimated parameters are accredited with the decision rule and the feedback is flooded into the network. Each node observes the transmission of other nodes. These observations are converted into measurable parameters.

Most of the detection schemes for misbehaving nodes have mainly three modules Observation module, Information sharing module and Decision making module. In the observation module, nodes observe activities of other nodes and record that information. Nodes make use of different techniques in observation module. They are: Passive acknowledgement: In this technique, nodes make use of overhearing mechanism help to know the other nodes transmissions. By overhearing neighboring nodes' transmissions, a node can understand whether its neighbor forwards its packet to other node without any hesitation. Active acknowledgement: This technique requires nodes to explicitly acknowledge the sender node about the successful reception of packet transmission. If an detail acknowledgement reaches the source node from the destination node. The node have forwarded the packets to destination if the source can make sure that all intermediate nodes in the transmission path are well behaved nodes.

In the information sharing module, all nodes are required to share the information collected by them with other nodes. Two kinds of information sharing are: Local sharing: A node shares its observations with its own neighbors alone. Global sharing: A node shares its observation with all nodes in the entire network.

ii. Control

Controlling the effect of misbehaving node involves the network nodes to communicate / spread the details of node misbehavior which they have already identified, with other neighbor nodes. This information can be made use of by other nodes for eliminating the misbehaving nodes in the future. Controlling the effect of misbehaving nodes can be in such ways.

Decreasing the level of misbehaving nodes in the network helps to increase the throughput and performance. Ad-Hoc networks have been an active area of research with lots of practical applications. Cooperation of all nodes in the network is of very much importance for achieving communication between nodes. MANETs are highly vulnerable to misbehaving nodes due to the absence of infrastructures, dynamically changing topology and open medium of communication.

Conclusion & future work

The various types of misbehaving nodes found in the network and the reasons for their misbehavior. An overall idea about misbehaviors at two layers of the OSI model; i.e., the network layer and MAC layer and a transient description of various existing schemes to detect the misbehaving nodes and to reduce the effect caused by them in the network is given in this paper. The Reputation based schemes mostly based on overhearing technique, have many complication and led the way to active acknowledgement based schemes. The credit based schemes requires the source node to keep the amount of essential money required for the transaction of the packet. These schemes impose a burden on the source node. Many other detection schemes were also proposed for the detection of misbehaving nodes. Merging the problems created by misbehaving nodes in various layers and finding out a cross layer based scheme for detection scheme is of further scope in this area.

It can be extended to resolve other network layer misbehavior such as control packet dropping.

References

[1] Debjit Dasa, Koushik Majumdera and Anurag Dasguptab "Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory", pp. 92-101, 2015

[2] Enrique Hernandez-Orallo, Manuel David Serrat Olmos, Juan-Carlos Cano,Carlos T. Calafate, and Pietro Manzoni "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 6, pp. 1162-1175, 2015

[3] Jebakumar Mohan Singh Pappaji Josh Kumar, Ayyaswamy Kathirvel*, Namaskaram Kirubakaran, Perumal Sivaraman and Muthusamy Subramaniam "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT", EURASIP Journal on WirelessCommunications and Networking, pp. 1-11, 2015

[4] Ming Li, Sergio Salinas, Pan Li, Jinyuan Sun and Xiaoxia Huang "MAC-Layer Selfish Misbehavior in IEEE 802.11 Ad-Hoc Networks: Detection and Defense", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOl. 14, NO. 6, pp. 1203-1217, 2015.

[5] *Naveen Kumar Gupta, **Ashish Kumar Sharma, ***Abhishek Gupta "Selfish Behavior Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)", International Journal of Research Review in Engineering Science and Technology, Volume-1 Issue-2, pp.31-34, September 2012

[6] Sengathir.J*, R. Manoharan "Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs", Egyptian Informatics Journal, pp. 231–241, 2015

[7] Santhosh J , Malini V K "A Heuristic Method against Selfish and Malicious Behavior Attacks in Opportunistic Networks", International Journal of Innovative Research in Computer And Communication Engineering, Vol. 4, Issue 3, pp. 4327-4333, March 2016

[8] Senthilkumar Subramaniyan*, William Johnson and Karthikeyan 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, pp. 1-10, 2014

[9] Priya.P, Gopinathan.B "Improving security based on detecting selfish nodes using MD5 encryption algorithm in MANETS", International journal of advanced technology in engineering and science, Vol. No.4, pp. 60-66 , 2016

[10] Virali Girdhar ,Gaurav Banga "A Incentive Based Scheme to Detect Selfish Nodes in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, pp. 561-565, August 2015