International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Implementation of Misbehavior Detection Approach in Wireless Ad Hoc Network

Vaijeshwari M. Waghmare[Á*] and Priyanka Fulare[Á]

[Á]CSE Department, RTM Nagpur University, India

Accepted 01 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

The network is created in wireless ad hoc fashion by involving nodes without any central administrator. In wireless ad hoc network there are no dedicated routers or network management nodes, but nodes work in peer to peer fashion and acts as both servers and routers. Since the nodes participate in the protocol execution as peers, any network node can abuse the protocol operation. It is difficult to identify the trustworthy nodes and misbehaving nodes. An approach is based on two parts for misbehavior detection in wireless ad hoc network. The first part detects the misbehaving links using the 2ACK algorithm and this information is transferred into second part which uses the principle of conservation of flow algorithm for detection of misbehaving node.

Keywords: *Ad hoc networks, Link misbehavior, Node misbehavior, Reputation system, Wireless communications.*

1. Introduction

Wireless ad hoc network is a collection of digital data terminals equipped with wireless transceivers which can communicate with each other without the need of any fixed infrastructure. Also the infrastructure based mobile networks like the cellular networks which require a base station for the transmission of data packets, the mobile ad hoc networks are infrastructure less networks where in the nodes can directly communicate with each other without the need of any routers (Shirina Samreen *et al*, 2012). Each node incorporates the functionality of the router and can transmit packets directly to those nodes which are within its transmission range and also forward packets on behalf of any other node which wishes to transmit the data packet to some other node which is not within its transmission range (Yu Zhang *et al*, 2012). In other words, to accomplish the data communication between those nodes which are not within the transmission range of each other, data packets are relayed over a sequence of intermediate nodes using the "store and forward multi-hop" transmission principle. In a wireless ad hoc network node can move freely and hence the topology is not fixed or static. The topology changes dynamically and has to be discovered by the nodes themselves either individually or collectively during the routing (Rahul Raghuvanshi *et al*, 2011; Sonja Buchegger, 2005). The nodes are also power-constrained and hence each node should ensure that it does not discharge its battery power.

In wireless ad hoc network, a node monitors the transmission of a neighbor to make sure that the neighbor forwards others traffic. If the neighbor does not forward others traffic, it is considered as uncooperative, and this uncooperative reputation is propagated throughout the network (Yanbin Liu *et al*, 2003). Although empirical evaluations have shown that the above systems can identify misbehaving nodes and improve the performance of an ad-hoc network, one important missing component is a formal analysis of the properties of the reputation systems.

According to an approach implemented when a node forwards a data packet, it expects to receive a 2ACK packet from the destination of the next hop link in wireless ad hoc network. Based on the number of packets which missed the 2ACK packets within a certain time limit, a decision about the misbehaving link is taken. This information of the misbehaving link is utilized by PFC algorithm which determines the misbehaving nodes associated with the misbehaving link. The decision is based on the analysis of inflow and the outflow of the data packets associated with the node. As pointed out in the 2ACK algorithm determines the misbehaving link and it has to be determined which one of the two nodes associated with this link are misbehaving (Shirina Samreen *et al*, 2012; Ahmet Burak Can and Bharat Bhargava, 2013). An approach works at determining the misbehaving node through the knowledge of misbehaving link by using the 2ACK algorithm followed by the PFC algorithm.

2. Related work

Yu Zhang, Loukas Lazos, William Jr. Kozma address the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks. Audit-based Misbehavior Detection (AMD) that

*Corresponding author: **Vaijeshwari M. Waghmare**

effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. As compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive.

Shirina Samreen, G.Narasimha has introduces approach which is based on the usage of two algorithm which will be used in parallel in such a way that the results generated by one of them are further processed by the other to finally generate the list of misbehaving nodes. The first part detects the misbehaving links using the 2ACK algorithm and this information is fed into the second part which uses the principle of flow of conservation (PFC) algorithm to detect the misbehaving node. K. Liu, J. Deng, P. Varshney and K. Balakrishnan improved on TWOACK by proposing 2ACK.

Rahul Raghuvanshi, Rekha Kaushik, Jyoti Singhai has introduces different mechanisms for detection and prevention of misbehavior node. Also, a check list provides a guideline to identify pros and cons of different mechanisms. Sonja Buchegger provided a scheme which extends the watchdog module to all one hop neighbors that can monitor nearby transmissions. When misbehavior is detected, monitoring nodes broadcast alarm messages in order to notify their peers of the detected misbehavior and adjust the corresponding reputation values. Similar, monitoring techniques have also been introduced by Q. He, D. Wu, and P. Khosla.

Yanbin Liu, Yang Richard Yang presents a formal specification and analysis of a general class of mechanisms to locally update the reputation of mobile nodes. Given an initial assessment of the reputation of other mobile nodes, formally show that under mild conditions, the mobile nodes will achieve reputation agreement.

3. Proposed research

3.1. Reputation module

The reputation module is responsible for managing reputation information based on the recommendations of the audit module. Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations. Nodes with low reputation values are excluded from routing paths, thus being unable to drop transit traffic in wireless ad hoc network. The reputation module is performing important work for computing and managing the reputation of nodes. Wireless ad hoc network adopt a decentralized approach in which each node maintains its own view of the reputation of other nodes (Sonja Buchegger, 2005). This type of implementation alleviates the communication overhead for transmitting information to a centralized location, and readily translates to the distributed nature of wireless ad hoc networks. Also, it allows nodes to hold individualized reputation metrics for their peers depending on their direct and indirect interactions (Meenakshi Patel *et al*, 2012). Here system has taken into account both first-hand and second-hand information. Information is considered to be first-hand if it is obtained by direct interaction between nodes (e.g., node n routes information via node m), and is considered to be second-hand if it is indirectly obtained based on the opinions of other nodes (Yu Zhang *et al*, 2012). Consideration of both first-hand and second hand information has been shown to improve the reliability of reputation metrics (Sonja Buchegger, 2005; Yanbin Liu *et al*, 2003; Xi Zhang *et al*, 2011). When a source S establishes a route to a destination D, the audit module running on S makes evaluations on the behavior of each node along the path. These evaluations are considered as first-hand information for S. The source propagates first-hand information to all nodes along path, thus providing second hand information (Yanbin Liu *et al*, 2003).

3.2. Route discovery module

The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination. This module is invoked by the source whenever there is no cached path to the destination. For identification of trustworthy routes, modify the discovery phase of the DSR protocol (Vasantha.V *et al*, 2007; Q. He *et al*, 2004). In DSR, when S has packets for D, it checks whether a route exists in its cache. If a route does not exist, S broadcasts a Route Request (RREQ) message. This message contains the source ID, destination ID, and the time to live (TTL). Any intermediate node that receives the RREQ appends its ID to the RREQ message and rebroadcasts it while decreasing the TTL field by one unit. If a receiving node is the destination, D responds to S with a route reply (RREP) message containing the entire path. The RREP follows the reverse path to S.

The failure of any one of component resulting as failure in entire system. On the other hand, failure of one of node results as a failure of entire path while routing. The node should work properly and analysis of node behavior is carried out on basis of 2ACK algorithm. The 2ACK algorithm has giving detection of misbehaving links from route discovery by dynamic source routing (DSR). The 2ACK algorithm is network layer algorithm. The 2ACK algorithm has executing with a triplet of node. As route is given by DSR from source to destination. From this route, nodes are differentiated into triplet of nodes. Consider a route established as S-A1-A2-A3-A4-D and triplets are given as (S-A1-A2),(A1-A2-A3),(A2-A3-A4),(A3-A4-D) after that 2ACK algorithm is applied. If (A2-A3-A4) is a set on which algorithm is applied, then A2 IS 2ACK sender and A4 is 2ACK receiver. If A2-A3 has not sending 2ACK then it is considered as misbehaving link. This information of misbehaving link is given to PFC algorithm for detection of misbehaving node.

3.3. Audit module

The identification of misbehaving node is carried out in audit module. The detection of misbehaving node is done with help of principle of flow of conservation (PFC) in wireless ad hoc network. Whenever a node forwards a data packet, it expects to receive a 2ACK packet from the

destination of the next hop link. Based on the number of packets which missed the 2ACK packets within a certain time limit, a decision about the misbehaving link is taken. This information of the misbehaving link is utilized by PFC algorithm which determines the misbehaving node associated with the misbehaving link. The decision is based on the analysis of inflow and the outflow of the data packets associated with the node given by PFC algorithm. As pointed out in the 2ACK algorithm determines the misbehaving link and it has to be determined which one of the two nodes associated with this link are misbehaving (Shirina Samreen *et al*, 2012; K. Liu *et al*, 2007). An approach works at determining the misbehaving node through the knowledge of misbehaving link by using the 2ACK algorithm followed by the PFC algorithm.

4. Simulation result

In wireless ad hoc network each node has running the 2ACK algorithm whenever a route has to be established from a source node S to a destination node D. The 2ACK algorithm involves the logical formation of overlapping triplets upon the routing path from source S to destination D. The route discovery module is executed by a node which is logically the first one in a triplet along the route. It forwards /sends the data packet and applies the concept of 2ACK algorithm to determine the misbehaving link.

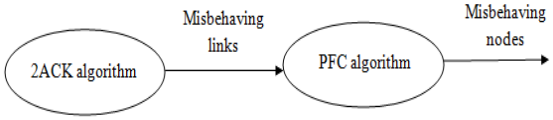

Fig 1 Working of an approach

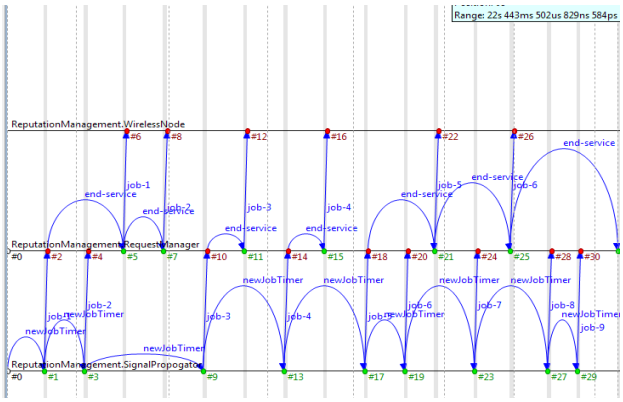

Fig 2 Execution of reputation module

The module 2ACK packet sender is executed by a node which is logically the last one in the triplet along a route given out by DSR. It receives the data packet and as per the 2ACK algorithm, if it is well behaving then, it is supposed to send 2ACK packet over two hops in the reverse direction to that node which is the first one in the triplet. Once a link is blacklisted, each of the nodes checks to see if any of their neighbors are associated with this link. The behavior check performs this task. It gathers the metrics associated with the neighbor node by broadcasting MREQ packets which stand for metrics request packet. It then sets a timer and starts waiting for MREP (metrics reply) packets from each of the associated neighboring nodes which are all accumulated. If all MREP packets are received, it checks to see if PFC condition is satisfied to arrive at a conclusion of whether the node being checked is well behaving or misbehaving. The sending of MREQ packets by behavior check module invokes another module called as metrics request handling. The audit module for PFC monitoring keeps running in background on each node to gather inflow and outflow metrics associated with each neighboring node in wireless ad hoc network.

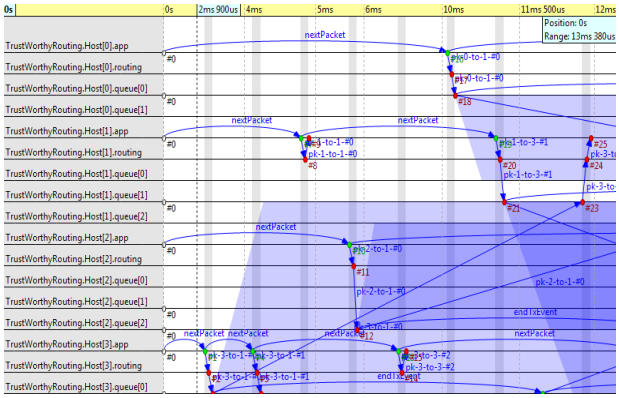

Fig 3 Execution of route discovery module

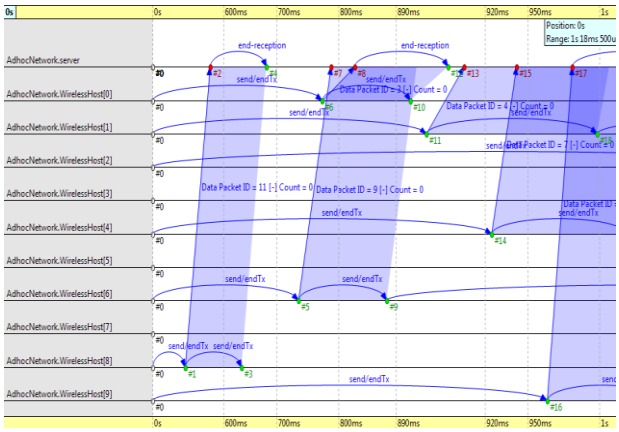

Fig 4 Execution of audit module

Conclusion

The implementation of an approach effectively and efficiently performs detection of misbehaving node by combination of 2ACK and PFC algorithm in wireless ad hoc network.

References

Yu Zhang, Loukas Lazos and William Jr. Kozma (2012), AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks, *IEEE transactions on mobile computing*, vol. x, no. x.

Shirina Samreen, G. Narasimha (2012), An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehaviour, *2013 3rd IEEE International Advance Computing Conference (IACC)*, pp.588-592.

Rahul Raghuvanshi, Rekha Kaushik , Jyoti Singhai (2011), A Review of Misbehaviour Detection and Avoidance Scheme in Adhoc Network, *IEEE,pp.301-306*.

Sonja Buchegger (2005), Self-Policing Mobile Ad Hoc Networks by Reputation Systems, *IEEE Communications Magazine*, pp.101-107.

Yanbin Liu, Yang Richard Yang (2003), Reputation Propagation and Agreement in Mobile Ad-Hoc Networks, *IEEE*, pp.1511-1515.

Q. He, D. Wu, and P. Khosla (2004), SORI: A secure and objective reputation-based incentive scheme for ad hoc networks , *IEEE Communications Society*, pp.825-830.

Vasantha.V,Dr.Manimegalai (2007), Mitigating Routing Misbehaviors using Subjective Trust Model in Mobile Ad hoc Networks, *IEEE*, pp.417-422.

Xi Zhang, Xiaofei Wang, Anna Liu, Quan Zhang and Chaojing Tang (2011), Reputation-based Scheme for Delay Tolerant Networks, *International Conference on Computer Science and Network Technology*, pp.974-978.

K. Liu, J. Deng, P. Varshney, and K. Balakrishnan (2007), An acknowledgment based approach for the detection of routing misbehavior in manets, *IEEE transactions on mobile computing*, vol. 6, no. 5.

Ahmet Burak Can,and Bharat Bhargava (2013), SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems, *IEEE transactions on dependable and secure computing*, vol. 10, no.1.

Meenakshi Patel, Sanjay Sharma (2012), Detection of Malicious Attack in MANET A Behavioral Approach, *2013 3rd IEEE International Advance Computing Conference (IACC)*, pp. 388-393.