IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 50-52
www.iosrjournals.org

A Review Of Misbehavior Detection Approach In Wireless Ad Hoc Network Based On Reputation

Vaijeshwari Waghmare[1], Priyanka Fulare[2], S. Patil[3]
[1,2]*Dept. of CSE, GHRIETW, RTM Nagpur, India*
[3]*Dept. of CSE, PCET, RTM Nagpur, India*
[1]vwaghmare2010@gmail.com, [2]priyanka.fulare@raisoni.net

ABSTRACT : *The problem of identifying and isolating misbehaving nodes that refuses to forward packets in wireless ad hoc networks. In this paper integration of reputation module, route discovery module and audit module are discussed. This system effectively and efficiently isolates both continuous and selective packet droppers. 2ACK and Principle of flow of conservation (PFC) techniques are used for detection of misbehaving link and misbehaving node simultaneously. The 2ACK technique detects the misbehaving link but it cannot decide which node is misbehaving from that link. Hence, that information from 2ACK technique is given to principle of flow of conservation (PFC) technique for detection of misbehaving node. As misbehaving nodes are listed from wireless ad hoc network route discovery is carried out by avoiding that misbehaving nodes.*

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

I. INTRODUCTION

In the absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. Moreover, selfish nodes may misconfigure their devices to refuse forwarding traffic in order to conserve energy [2], [3]. This type of behavior is known as node misbehavior. Existing solutions for identifying misbehaving nodes either use some form of per-packet evaluation of peer behavior [4], [9].

On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing [4], [5] or achieving of per-packet acknowledgement [9]. This type of monitoring operations must be repeated on every hop of a multihop route, thus it require high communication overhead and energy expenditure. Also, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected. Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes and reputation values are given to node according to its functionality of packet forwarding [4], [5], [8].

Objectives are

- Provide an effective mechanism to deal with misbehaving nodes in the network
- Effectively and efficiently detection of both continuous selective packet dropping
- Encourage co-operation among nodes in the network
- Minimize computation overhead at each node
- Detection of misbehaving link and node in parallel
-

II. RELATED WORK

Yu Zhang, Loukas Lazos, William Jr. Kozma [1] 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 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 [2] has introduces approach which is based on the usage of two techniques 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 technique and this information is fed into the second part which uses the principle offlow of conservation (PFC) technique to detect the misbehaving node. K. Liu, J. Deng, P. Varshney and K. Balakrishnan [9] improved on TWOACK by proposing 2ACK.

Rahul Raghuvanshi, Rekha Kaushik, Jyoti Singhai [3] 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 [4] 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 [6].

Yanbin Liu, Yang Richard Yang [5] 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.

III. SYSTEM MODEL

3.1 AMD system architecture:

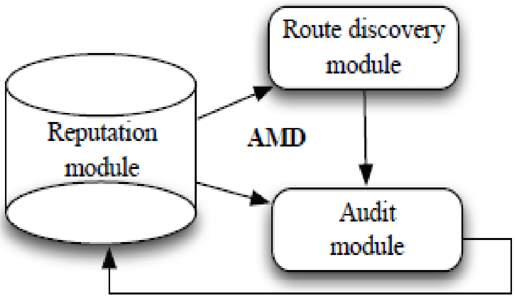

Fig. 1: AMD system architecture

3.1.1 The reputation module:

The reputation module is responsible for computing and managing the reputation of nodes. It adopts a decentralized approach in which each node maintains its own view of the reputation of other nodes on basis of first hand information or second hand information [6]. Such implementation alleviates the communication overhead for transmitting information to a centralized location, and readily translates to the distributed nature of wireless ad hoc networks. Nodes with low reputation values are excluded from routing paths.

3.1.2 The route discovery module:

The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination. There is no universal reputation value for each node, but the reputation values are individual perceptions of trustworthiness of one node in regards to another.

3.1.3 The audit module:

The audit module is responsible for identifying the set of nodes that misbehave in a particular path. The source invokes the audit module if it detects poor performance on path. The exact definition of what constitutes poor performance can be determined on the basis of a packet forwarding between source and destination. One possible mechanism for determining the path performance is to monitor the average end-to-end packet rate overa window of time. If packet rate is less than threshold per second, the audit module is activated. The threshold is source-defined and can be statistically derived based on prior interactions of the source with other destinations, or some minimum expected network performance.

These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers. A schematic of the relationship between the three modules of AMD as shown in above figure.

3.2 An efficient approach:

The approach is based on the usage of two techniques 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.

3.2.1 2ACK technique:

It can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving. Each node keeps running the 2ACK algorithm whenever a route has to be established from a source node S to a destination node D. The 2ACK technique involves the logical formation of overlapping triplets upon the routing path from source S to destination D. It receives the data packet and as per the 2ACK technique, 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.

3.2.2 Principle of flow of conservation (PFC) technique:

PFC for the second part which detects the misbehaving nodes associated with that of the misbehaving link. Once a link is blacklisted by the 2ACK technique, the PFC technique takes both nodes associated with that link as input and finds out behavior of both nodes individually. The misbehaving nodes are all blacklisted so that such nodes can be penalized by not involving it in any sort of network activity. PFC gives direct relation exists between the rate of inflow traffic and the rate of outflow traffic associated with a node.

IV. CONCLUSION

AMD can detect selective dropping attacks over end to-end encrypted traffic streams. The 2ACK technique detects the misbehaving link but cannot decide which one of the two associated nodes are misbehaving, hence by applying PFC technique as the next step to detect the misbehaving nodes once the misbehaving link is detected. The computational overhead by PFC technique is reduced as examining only those nodes behavior which are associated with misbehaving links.

References

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

[2] Shirina Samreen, G. Narasimha. "An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehaviour", 2013 3rd IEEE International Advance Computing Conference (IACC), IEEE 2012.

[3] Rahul Raghuvanshi, Rekha Kaushik , Jyoti Singhai. "A Review of Misbehaviour Detection and Avoidance Scheme in Adhoc Network" , IEEE 2011.

[4] Sonja Buchegger. "Self-Policing Mobile Ad Hoc Networks by Reputation Systems", IEEE Communications Magazine, July 2005.

[5] Yanbin Liu, Yang Richard Yang. "Reputation Propagation and Agreement in Mobile Ad-Hoc Networks",IEEE 2003.

[6] Q. He, D. Wu, and P. Khosla. "SORI: A secure and objective reputation-based incentive scheme for ad hoc networks", IEEE 2004.

[7] Vasantha.V,Dr.Manimegalai.D. "Mitigating Routing Misbehaviors using Subjective Trust Model in Mobile Ad hoc Networks", IEEE 2007.

[8] Xi Zhang, Xiaofei Wang, Anna Liu, Quan Zhang and Chaojing Tang." Reputation-based Scheme for Delay Tolerant Networks", International Conference on Computer Science and Network Technology, IEEE 2011.

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

[10] Ahmet Burak Can,and Bharat Bhargava. "SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems", IEEE transactions on dependable and secure computing, vol. 10, no.1, January/February 2013.

[11] Meenakshi Patel, Sanjay Sharma. "Detection of Malicious Attack in MANET A Behavioral Approach", IEEE 2012.