ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

Detecting Truthfulness and Preserving Privacy in Data Packet Dropping Through Malicious Codes in WANETs

T.Shiva Krishna[1], Vadlamudi Muniraju Naidu.[2]

PG Scholar, Dept. of CSE, Narayana Engineering College, Nellore, AP, India[1]

Associate Professor, Dept. of CSE, Narayana Engineering College, Nellore, AP, India. [2]

.

ABSTRACT: Multi-hop wireless ad-hoc network (WANET) gives increase in coverage and provide more beneficiary over traditional wireless local area networks. However this architecture is more vulnerable in dealing with attacks internally from nodes which are compromised. One of them is packet dropping attack which is a very considerable in issue of networking. Link error and malicious packet dropping are two sources for packet losses. While observing a continuous packet loss in the network, it's hard to identify whether the loss is due to link errors or malicious ones. This research paper focuses on insider-attack scenario, whereby malicious nodes that are part of the route selectively drop a little amount of packets which are essential to the performance of the network. The malicious node may identify the importance of different packets and drops few of them which are important to the network operation. Since packet dropping rate in this case is comparable to the channel error rate, existing detection algorithms cannot achieve satisfactory detection accuracy in identifying packet loss rate. Improvement in Detection accuracy can be done by exploiting the correlations among packets lost. In this research paper, a public auditing is applied which allows the detector to find the truth about the packet loss information. The proposed technique is preserves privacy, collusion proof, and it incurs low communication and storage overheads at intermediate nodes. And also achieves better detection accuracy than the conventional methods such as a maximum likely detection.

KEYWORDS: Packet Dropping, Auditing, Attack Detection, Secure Routing, truthfulness in packet drops, accurate detection of packet drops, wanet packet drop detection.

I. INTRODUCTION

In a multi-hop network, nodes will cooperate in relaying/routing traffic. An adversary can exploit this cooperative nature to do attacks. As an example, the adversary will first pretend to be a cooperative node in the route discovery method. Once entered in a route, the adversary node starts dropping packets. In the most severe form, the malicious node will stop forwarding all packets that receives from upstream nodes, completely disrupting the path between the source and destination. Actually, such a strong Denial-of-Service (DoS) attack can paralyze the network by partitions the topology.

There are various reasons for packet losing which is shown in fig.1. A malicious node that is part of the route will explore its knowledge about the network policy and the communication context to launch an insider attack–which is intermittent, but can have similar performance degradation effect as a persistent attack at a much lower risk detecting frequently. Eventually, the malicious node can evaluate the importance of various packets, and then drop the little amounts that are highly critical to the operation of the network. For example, in a frequency-hopping network, those are the packets that express frequency hopping sequences for network-wide frequency-hopping synchronization; in an ad hoc radio network, they may be the packets that carry the idle channel lists (i.e., white spaces) which are used in establishment of a network-wide channel control. By targeting these highly critical packets, intermittent insider attacks may cause considerable damage for network with low probability of being caught. In this paper, we are enthusiastic to defend such insider attacks. In particular, we are interested in the problem of detecting the occurrence of selected packet droppings and identify the malicious node which is responsible for these drops.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

In this paper, we develop an algorithm which is accurate for detecting selective packet drops made by insider attackers. Our algorithm also provides a truthful and verified decision statistics as a proof to support the detection decision.

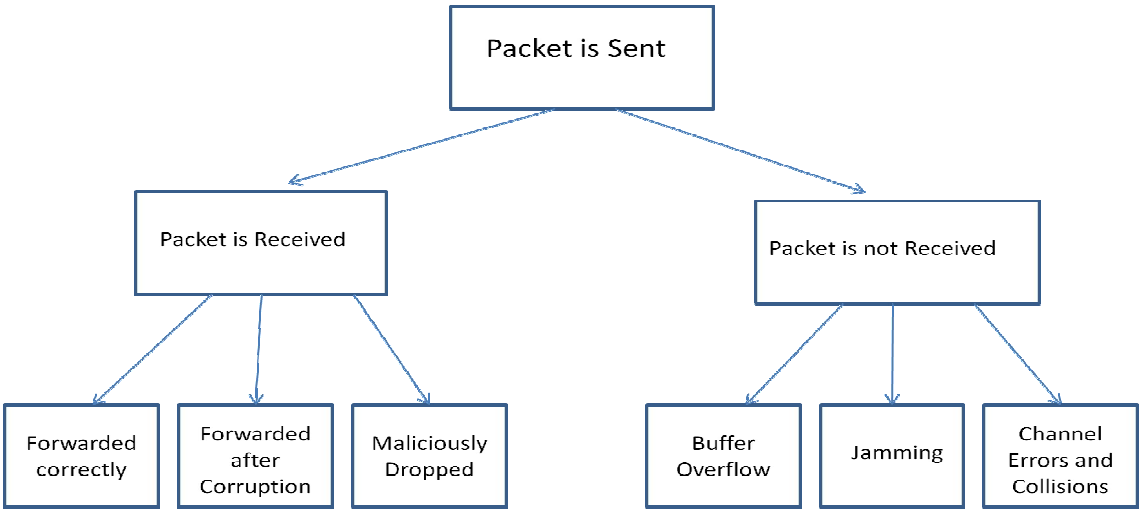


Fig. 1: Overview of Packet Loss

A. Problem Statement:

Detection of selected packet-dropping attacks is widely challenging in a highly dynamic environment. The hardness will be from the requirement that we need to not only detect the place of packet drop, but also find that the drop is intentional or unintentional. Specifically, due to the openness of wireless source, the packet drop in the network could be caused by rough channel conditions (e.g., fade, noise and interfering, link error), or by the insider attacker. In an open wireless environment, link errors are important, and will not be significantly smaller than the packet dropping rate of the insider attacker. Here the detection must be done by the public auditor that does not have knowledge of the data held by the nodes on the network route. When a malicious node is identified, the auditor should be able to construct a proof of the misbehavior of that node.

II. RELATED WORK

The related work on the detection of packet dropping attacks can be classified into two categories.

A. The first one aims at huge malicious dropping rates, where most (or all) lost packets are caused by malicious droppings. The impact of link errors is ignored in this case.

Most related work falls into this category. Based on the methods used to find the attackers, these works can be further classified into four sub-categories. The first one is on credit systems. A credit system provides an incentive for cooperation. A node receives credit on relay of packets, and uses that credit to send its own packets. As a result, a maliciously node that continuously drop packets that eventually deplete its credit, and will not be able to send its own traffic. The second one is on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving ones. The node with a high packet dropping rate is founded with a bad reputation by its neighbors. This reputation information is transmitted in periodical fashion throughout the network and is used as an important metric in selecting routes. Sequentially, a malicious one will be removed from any route. The third sub-category of works relies on end-to-end acknowledgement that directly locates the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

B. The second one aims in the scenario where the number of maliciously dropped packets is more than the packets dropped by link errors, but the influence of link errors is non-negligible.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

Limitations:

1) In the credit-system-based method, a malicious node may still receive enough credits by relaying most of the packets that received from up nodes.
2) The reputation approach, the malicious node can maintain a reasonably good reputation by sending much more packets to the next hop.
3) For the acknowledgement-based method and all the mechanisms in the second scheme, counting of lost packets does not give a sufficient ground to detect the real attacker causing packet loss.

III. PROPOSED SYSTEM

The proposed method is based on detecting the correlations among the losed packets over every hop in the path. It gives a truthful and publicly verifiable decision statistical analysis as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations among the positions of lost data, as calculated by the auto-correlation function (ACF) which describes the status of every packet in continuous of packet transmission. Therefore, by detecting the correlations between the lost packet, which can decide the reason for the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error.

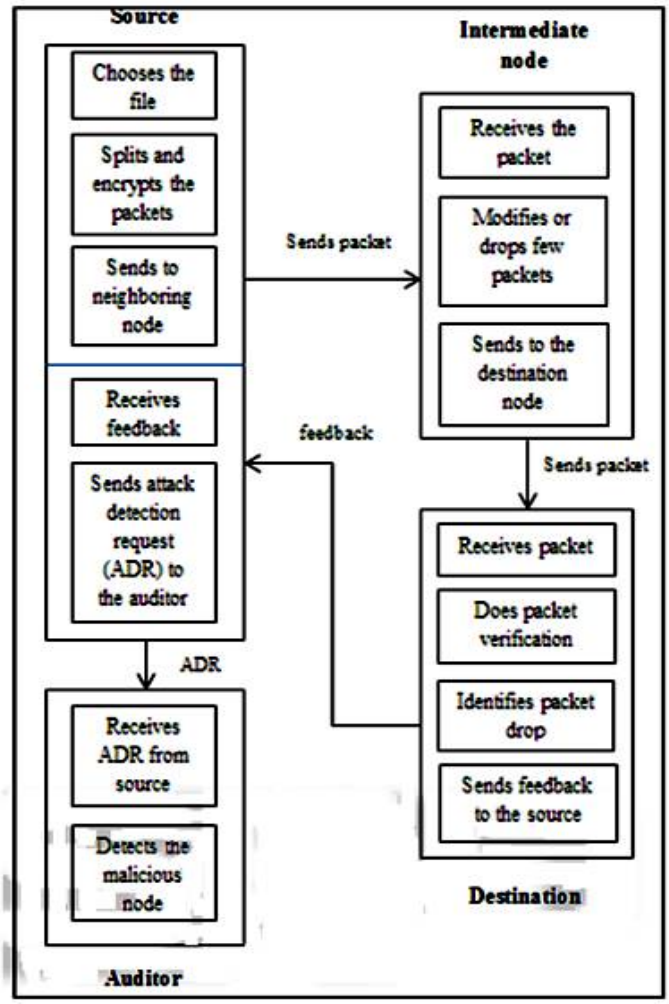


Fig. 2: Proposed Architecture

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

A. Network Model:

The wireless channel as shown in below figure 3., in which the source node stream line the packets to the destination through intermediate nodes n1……nk (where ni is the upstream node of ni+1). is modeled of each hop along P (Path to Source and Destination) as a random process that alternates among good and bad states. Packets transmission during the good state is successful, and packets transmitted during the bad state will lost. M packets is transmitted over the channel.

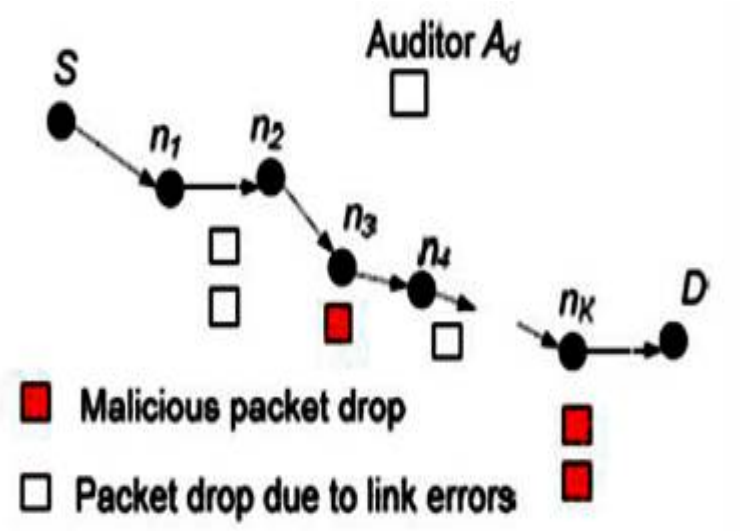


Fig. 3: Network and Attack Model

B. Independent Auditor:

Here we have an independent auditor in the network. Ad is independent in the sense that it is not associated with node in P. The auditor is meant for detecting malicious nodes on demand. Specifically, it is assumed S will get feedback from D where D suspects that the route is under attack. After receiving feedback, S sends ADR to Ad, Ad begins to identify the packet loss. To facilitate its investigation, Ad needs to collect certain information from the nodes on the route.

C. Setup Phase:

In this phase takes place immediately after path P is established, but before any packets transmitted in the route. In this phase, Source node encrypts the packet and sends to destination via intermediate nodes. on receiving the packets destination node can verify the packets and after verification the packets are decrypted.

D. Advantages in Proposed work:

1) High detection accuracy.
2) Privacy preserving.
3) Low communication and storage overheads.

IV. EXPERIMENTAL ANALYSIS

1. To compare the detection accuracy achieved by the proposed algorithm with the optimal maximum likelihood algorithm, which only utilizes the distribution of the number of lost packets.
2. For given packet-loss bitmaps, the detection on different hops is conducted separately.
3. So, simulated the detecting a hop for performance evaluation of a given algorithm.
4. So, assumed that packets are transmitted continuously over this hop, i.e., a saturated traffic environment.
5. Transition probabilities from good to bad and from bad to good given by PGB and PBG.
6. Two types of malicious packet dropping: random dropping and selective dropping.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

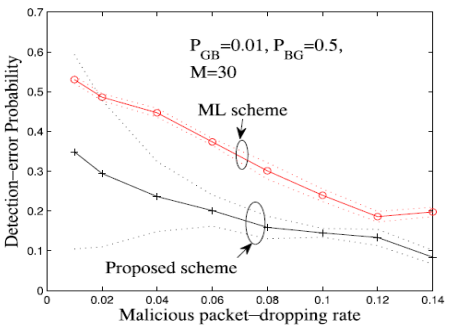
An ISO 3297: 2007 Certified Organization Vol.4, Special Issue 1, April 2016

International Conference on Computational Intelligence (ICCI - 2016)

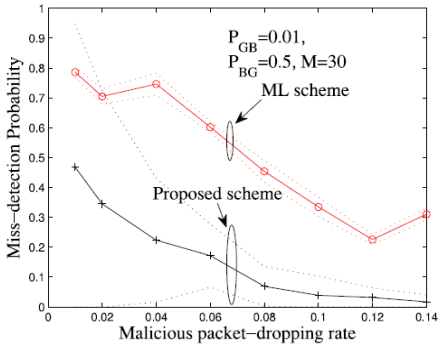
On 23rd April 2016, Organized by

Dept. of CSE, Narayana Engineering College, Nellore, India

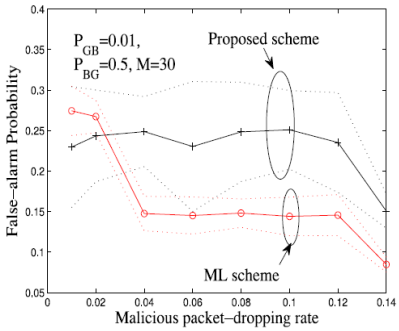
7. In the random dropping attack, a packet is dropped at the malicious node with probability PM. In the selective droppings, the adversary packets of specific sequence numbers.



(a) Overall detection-error probability



(b) Miss-detection probability



(c) False-alarm probability

V. CONCLUSION

It is compared with conventional detecting algorithms which uses only the distribution of the number of lost packets, exploiting the correlation among lost packets drastically improves the accuracy in detecting malicious packet drops. Such improvement is highlighted if the count of maliciously dropped packets is comparable with those caused by link errors. To exact calculation of the correlation among lost packets, it is critical to acquire truthful packet-loss information at every individual node. Created a Public auditing system which ensures truthful packet-loss reporting by individual nodes. This architecture is proven collusion proof, which requires high computational capacity at the source node, which incurs in low communication and storage overhead in the route.

REFERENCES

[1] A. Proano and L. Lazos. Packet-hiding methods for preventing selective jamming attacks. IEEE Transactions on Dependable and Secure Computing, 9(1):101–114, 2012.
[2] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim. Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In Proceedings of the IEEE ICC Conference, 2009.
[3] M. Kiran kumar and A. Sai harish. A novel schema for detecting malicious packet losses. International journal of modern engineering research, 2012.
[4] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing. In Proceedings of the IEEE INFOCOM Conference, Mar. 2010.
[6] M. Just, E. Kranakis, and T. Wan, ―Resisting malicious packet dropping in wireless ad hoc networks,in In Proc. of ADHOCNOW03. Springer Verlag, 2003, pp. 151–163.
[7] F. Anjum and R. Talpade, ―Lipad: lightweight packet drop detection for ad hoc networks,‖ Vehicular Technology Conference, 2004. VTC2004- Fall. 2004 IEEE 60th, vol. 2, pp. 1233–1237 Vol. 2, Sept. 2004
[8] O. F. Gonzalez, M. P. Howarth, and G. Pavlou, ―Detection of packet forwarding misbehavior in mobile ad-hoc networks.‖ in WWIC,ser. Lecture Notes in Computer Science, F. Boavida, E. Monteiro,

BIOGRAPHY

T.Shiva Krishna has received his B.Tech degree in Computer science and Engineering from Geethanjali Institute of Science and Technology Engineering college affiliated to JNTU, Anantapur in 2013 and pursuing M.Tech degree in Computer science and Engineering in Narayana College of Engineering affiliated to JNTU, Anantapur in 2014-2016.

Vadlamudi Muniraju Naidu has received his B.Tech in Computer Science and Engineering from SVCET Chittoor, JNTUH, 2005 and M.Tech degree in Computer science and Engineering from Nagarjuna University in 2010. He is dedicated to teaching field from the last 10 years. He has guided 5 P.G and 11 batches U.G students. His research areas included Networks. At present he is working as Associate Professor in Narayana Engineering College, Nellore, Andhra Pradesh, India.