IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 24-26
www.iosrjournals.org

Well-Organized Privacy Preserving and Corrupted Packet Dropping in Networks

Shilpa Ann Varghese[1], Devi Dath[2]
[1](Department of Computer Science, College of Engineering Perumon, India)
[2](Department of Computer Science, College of Engineering Perumon, India)

Abstract: *In the case of networks, security is always a serious concern. It is required to provide proper security to the network to safeguard them. Link Errors and Corrupted Packets are the two main issues, where Packet dropping is one of the serious issue. When a packet loss happens, we have to check whether it happened only due to the Link Error or it happened with the combination of Link Error and Corrupted Packets. In this paper we are focusing on insider attack. To boast the correctness of detection, we have to consider the connection between the missing packets. To safeguard truthful calculation of connection, we will develop a Homomorphic Linear Authenticator (HLA).*

Keywords: *Attack Identification, Corrupted Packet, Homomorphic Linear Authenticator, Link Error, Packet Missing.*

I. Introduction

In networks, the nodes collaborate to create traffic. The corrupted node does not forward every packet received from other nodes. It also distorts the path of packet from source to destination. The topology partition is done by Denial-of-Service attack which disables the network. The presence of high count of missing packets and corrupted nodes in a network, helps to identify the attack easily. If we are able to identify the corrupted nodes, we can use the Routing table to eliminate the corrupted node from the list. The corrupted node in a route creates insider attack in networks. In this paper, we will be solving the problem by detecting the corrupted nodes and the packet loss. Most of the times, the packet loss in channels are caused due to common conditions such as fading, noise, involvement etc. Link layer in a network is responsible for communication between the adjacent networks. Communication failure happens if there is any error. The packet loss rate is not enough to completely identify the reason for packet loss. In this paper, we develop an efficient algorithm to detect discriminating packet loss made by insider attack. The effective accuracy is achieved by considering the connection between the lost packets, it is calculated by using the Auto-Correlation Function (ACF).

II. Existing System

Traffic patterns are observed for the detection of packet loss. Traffic intensity are checked by using sensors. This paper suggests a traffic transmission pattern to be selected and the identification is done by the receiver. This is a common technique for intrusion detection but it is not bandwidth limited, so it cannot be implemented in a bandwidth limited network [1].

A Self Organizing mechanism is used to split the node for transmission in network. This technique helps node for active participation. This mainly focuses on enhancement of the connectivity of broke nodes in networks [2]. The detection of jamming attack in networks finds out the radio interference attacks. This study proposes two detection protocol that hire consistency checking. The feasibility and effectiveness of jamming attacks and its detection is considered in this study [3].

A secure routing protocol is presented to overcome the problem of colluding attackers in secure wireless routing. Secure routing protocol, Sprout1 continuously selects alternative routes to the destination [4].

The problem for scrutinizing and recognizing the misbehaving nodes are considered. These nodes refuse to forward the packets. The resource-efficient account-ability for node misbehavior is identified by the new misbehavior identification scheme called REAct [5]. A multipath scheme for "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Route" was implemented. This work acquires a routing algorithm, which computes the same route that is known for source. This paper develops a mechanism that generates randomized multipath routes [6].

A packet hiding method used as prevention from selective jamming attack was developed. The problem of jamming under the internal threat model is considered here. The adversary is aware of network secrets and implementation details of network protocol [7].

"Packet Drop Attack Detection Technique in Wireless Adhoc networks: a review" provides various technique based on reputation module, route discovery module, audit modules referred as the AMD system [8].

A model called Provable Data Possession (PDP) has been introduced that store data in skeptical server to ensure that the server has the original data without retrieving it. The proposed model produces a probabilistic proof of control from the server by sampling the random sets of blocks that hardly reduces I/O cost [9].

For a client, Proofs of Storage (PoS) acts as mutual protocols; to verify that a server stores a file reliably. This work provides a framework for creating HLA from identification protocol. A framework is proposed for generating public key HLAs based on certain identification protocol which satisfies homomorphic properties [10].

III. Proposed System

The drops are caused due to the insider attack. To overcome the difficulties of the packet drop, we develop an accurate algorithm for detecting the selective packet drops to achieve high identification accuracy. The position of the missing packet is identified by using an Auto-Correlation Function (ACF). The bitmap calculation helps to find out the status of the packets. If we analyze the correlation between the missing packets, we can confer whether the packet loss is due to the result of Link Error or Corrupted packet. The truthfulness for the correlation between missing packets are very important, for this auditing is done. A public auditing is established based on Homomorphic Linear Authenticator (HLA). We should also check the truthfulness of the source node and destination node.

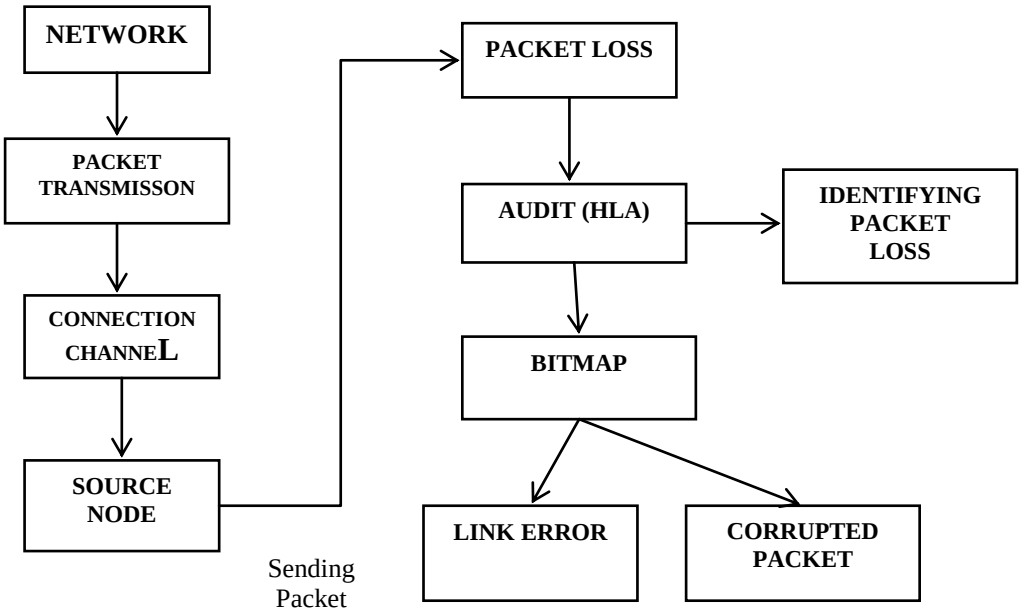

Fig 1: System Architecture

IV. Conclusion

Identifying the corrupted packets in the network is a challenging task. Utilizing the correlation of missing packets we identify the packet loss happened due to Link Error or Corrupted packets. This approach provide high identification accuracy. The truthfulness of source node and destination node is also considered in this work. This proposed system has high accuracy and it is privacy preserving.

Acknowledgements

We thank members of Computer Science and Information Technology department of College Of Engineering, Perumon for their valuable support and feedback

References

[1] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," *in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.*

[2] L. Buttyan and J. P. Hubaux. "Stimulating cooperation in self-organizing mobile ad hoc networks". *ACM/Kluwer Mobile Networks and Applica- tions, 8(5):579–592, Oct. 2003.*

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.*

[4] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," *in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.*

[5] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," *in Proc. ACM Conf. Wireless Netw. Secur. 2009, pp. 103–110.*

[6] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.*

[7] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Trans. Depend. Secure Comput. vol. 9, no. 1, pp. 101–114, Jan. /Feb. 2012.*

[8] "Secure routing and attack detection in wireless ad hoc network",*vol 1, oct 2014*

[9] J. N. Arauz, "802.11 Markov channel modeling," *Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.*

[10] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," *in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.*