IJRRECS/November 2015/Volume-3/Issue-11/4918-4923 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

TOWARDS RECOGNITION OF MALICIOUS NODES LIABLE FOR SELECTIVE PACKET DROPS

Suneetha Thaduri [1], Suneela Tharagaturi[2], V.Harsha Shastri[3], K.Anitha[4]

[1]Lecturer, Dept of CS, Loyola Academy Degree and P.G College, Secunderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Guru Nanak Engineering College, Hyderabad, T.S, India

[3]Lecturer, Dept of CS, Loyola Academy Degree and P.G College, Secunderabad, T.S, India

[4]Lecturer, Dept of CS, Loyola Academy Degree and P.G College, Secunderabad, T.S, India

ABSTRACT:

In our work we are concerned in detecting problem of selective occurrence of packet drops and identification of malicious nodes that are accountable for these drops. Identification of selective attacks of packet-dropping is very much challenging in extremely active wireless environment. The complexity comes from prerequisite that we need to detect place where packet is dropped, but moreover recognize whether drop is intended or else unintended. We build up a method of homomorphic linear authenticator that is based on public auditing design that permits detector to make sure reliability of packet loss data which is reported by nodes. This construction is privacy preserving, collusion proof, as well as acquires low communication along with storage overheads. The projected linear authenticator primitive is a signature system that is extensively employed within cloud computing as well as storage server systems to make available a proof of storage from server towards entrusting clients. In our work while examination of packet loss sequence within the network, we are concerned in determining whether losses are caused by means of link errors, or else by collective effect of link errors.

Keywords: Wireless environment, Cloud computing, Malicious nodes, Homomorphic linear authenticator, Privacy preserving, Signature, Link errors, Selective attacks.

1. INTRODUCTION:

Based on the weight an algorithm of detection gives to link errors in relation to malicious packet drops, related efforts are of two categories. The initial category intends at extreme malicious dropping rates, in which most of the lost packets are caused by means of malicious dropping [1]. Most of the works relates to this category. The other one target the situation in which several malicious dropped packets is considerably advanced than link errors, however link errors impact is non-negligible. A malicious node is a route part which exploits its network protocol data and communication circumstance to commence an insider attack which is intermittent, but attains similar effect of performance degradation as a constant attack at low threat of being detected. Most importantly, malicious node might assess various packets, and subsequently drop minute amount that are considered extremely important towards network operation. In our work we are concerned in combating the insider attack. Because of open wireless medium, packet drop within the network might be caused by means of conditions of harsh channel, or else by insider attacker. In the open wireless setting, link errors are relatively important, and might not be less important than the rate of packet dropping of insider attacker. Hence insider attacker camouflage in background of conditions of harsh channel. In this situation, by means of observing rate of packet loss is not sufficient to recognize exact cause of packet loss [2][3]. For improvisation of detection accurateness, we suggest to make use of correlations among lost packets. We develop a method of homomorphic linear authenticator that is based on public auditing design that permits detector to make sure reliability of packet loss data which is reported by nodes. Homomorphic linear authenticator primitive is a signature system that is extensively employed within cloud computing as well as storage server systems to make available a proof of storage from server towards entrusting clients. The proposed construction is privacy preserving, collusion proof, as well as acquires low communication along with storage overheads.

2. METHODOLOGY:

In our work while observation of packet loss sequence within the network, we are concerned in determining whether losses are caused by means of link errors, or else by

collective effect of link errors. We are concerned in the case of insider-attack, where malicious nodes the exploit their data of communication circumstance to drop a little mount of packets important towards network performance. The most important challenge in our method is in assuring that packet-loss bitmaps that are reported by particular nodes all along route are honest and such reliability is necessary for accurate calculation of correlation among lost packets. This challenge is not trivial, since it is normal for an attacker to report fake data to detection algorithm to keep away from being detected. Hence an auditing method is essential to confirm honesty of reported information. Although malicious dropping might effect in packet loss rate that is similar towards regular channel losses, stochastic process that distinguish two phenomena will display distinctive correlation structures. In our work we develop an accurate algorithm for detection of selective packet drops that are made by means of insider attackers. For enhancing of detection accurateness, we put forward to make use of correlations among lost packets. We build up a method of homomorphic linear authenticator that is based on public auditing design that permits detector to make sure reliability of packet loss data which is reported by nodes [4]. It is a privacy preserving, collusion proof, as well as acquires low communication along with storage overheads. Our structure provides honest as well as verifiable decision statistics to support recognition decision. The proposed linear authenticator primitive is a signature system that is extensively employed within cloud computing as well as storage server systems to make available a proof of storage from server towards entrusting clients. Direct usage of homomorphic linear authenticator is not the solution since in the problem setup, there might be more than single malicious node all along the route. These nodes may possibly collude throughout the attack and during the submission of reports.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Our study will target demanding circumstance in which link errors as well as malicious dropping will lead towards equivalent packet loss rates. The attempt in the literature on this difficulty was relatively preliminary, and there are only some related efforts. Cryptographic methods projected to counteract selective packet jamming aim a separate problem than detection. In our work

we build up a precise algorithm for detection of selective packet drops that are made by means of insider attackers. We build up a method of homomorphic linear authenticator that is based on public auditing design that permits detector to make sure reliability of packet loss data which is reported by nodes. Homomorphic linear authenticator primitive is a signature system that is extensively employed within cloud computing as well as storage server systems to make available a proof of storage from server towards entrusting clients. The challenge in our method is in assuring that packet-loss bitmaps that are reported by particular nodes all along route are honest and such reliability is necessary for accurate calculation of correlation among lost packets. It is not trivial, since it is normal for an attacker to report fake data to detection algorithm to keep away from being detected hence an auditing method is essential to confirm honesty of reported information. The system is privacy preserving, collusion proof, as well as acquires low communication along with storage overheads [5]. Our system provides honest as well as verifiable decision statistics to support recognition decision. The high detection accurateness is by means of exploiting correlations among positions of missing packets, as calculated from the function of auto-correlation concerning packet-loss bitmap. The fundamental thought behind our system is that although malicious dropping might effect in packet loss rate that is similar towards regular channel losses, stochastic process that distinguish two phenomena will display distinctive correlation structures. Hence by means of detection of correlations among lost packets, one can come to a decision whether packet loss is because of normal link errors, or else is a mutual effect of link error as well as malicious drop [6]. Our system will consider cross-statistics among lost packets to build additional informative decision, and as a result is in sharp difference towards traditional techniques that depend only on distribution of lost packets.

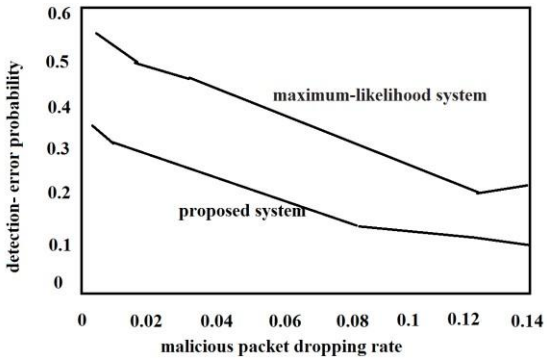

Fig1: An overview of overall detection error possibility.

4. CONCLUSION:

In severe form, malicious node will stop forwarding of each packet that is received from upstream nodes, totally disruption of path among source as well as destination. Such denial-of-service attack can paralyze network by means of partitioning topology. In our work we develop an accurate algorithm for detection of selective packet drops that are made by means of insider attackers. For managing detection accurateness, we suggest to make use of correlations among lost packets we develop a method of homomorphic linear authenticator that is based on public auditing design that permits detector to make sure reliability of packet loss data which is reported by nodes. Homomorphic linear authenticator primitive is a signature system that is extensively employed within cloud computing as well as storage server systems to make available a proof of storage from server towards entrusting clients. While inspection of packet loss sequence within the network, we are concerned in determining whether losses are caused by means of link errors, or else by collective effect of link errors. The significant challenge in our method is in assuring that packet-loss bitmaps that are reported by particular nodes all along route are honest and such reliability is necessary for accurate calculation of correlation among lost packets. This challenge is not trivial, since it is normal for an attacker to report fake data to detection algorithm to keep away from being detected. Hence an auditing method is essential to confirm honesty of reported information. Our scheme will consider cross-statistics among lost packets to build additional informative decision, and as a result is in sharp difference towards traditional techniques that depend only on distribution of lost packets. The proposed system arrangement is privacy preserving, collusion proof, as well as acquires low communication along with storage overheads.

REFERENCES

[1] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventingselfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[3] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Dec. 2008, pp. 90– 107.

[5] 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.

[6] T. Shu, S. Liu, and M. Krunz, "Secure data collection in wireless sensor networks using randomized dispersive routes," in Proc. IEEE INFOCOM Conf., 2009, pp. 2846–2850.

Suneetha Thaduri is Working as Lecturer in Computer Science in Department of Computer Science, Loyola Academy Degree and P.G College, Old Alwal, Secunderabad, Telangana - 500010, India. She has received her M.Tech in Computer Science and Engineering from Osmania University, University College of Engineering, Hyderabad, Telangana., India. Her research areas include Cloud Computing, Grid Computing, Green Computing, Mobile Computing, Data Mining, Networking and Image Processing.

Sunila Tharagaturi, MCA, Interested Areas include Operating systems, Cloud computing, Mobile Computing. Assistant Proffessor at Guru Nanak Engineering College.

V.HarshaShastri, M.Tech(CSE), Lecturer in Computer Science, Loyola Academy Degree and P.G College, Old Alwal, Secunderabad- 500010. Interested Areas include Mobile Computing, Operating Systems.

K.Anitha, Lecturer in Computer science and Engineering, Loyola academy degree and P.G College, Alwal,Secunderabad. Her interest areas include c,c++, java.