isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 Apr,2016,ISSN_NO: 2320-7248

DETECTING PACKETS IN WIRELESS ADHOC NETWORK

R.Jothi*, S.Loga Priya*,A.Kinnera Sai*,Dr.S.Padma Priya*(Professor)
Computer Science and Engineering
Prathyusha Engineering College Tiruvallur
rjothivyshali@gmail.com Priyaloga16@gmail.com

Abstract— The sequence of packets losses in the network ,we are interested in determining whether the losses are caused by link error only or combined effects of link error and malicious drop. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between loss packets. To ensure truthful calculation of this correlations, we develop a Homomorphic Linear Authenticator (HLA) based public auditing architecture that allow the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. We verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

Keywords—packet dropping,homomorphic linear authenticator(HLA),public auditing.

INTRODUCTION

Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirements that we need to not only detect the place where the packets is dropped ,but also identify whether the drop is intentional or unintentional. Specifically, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions .The accurate algorithm for detecting the selective packet drop made by insider attacks. Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy by exploiting the correlations between the positions of lost packets, as calculated from the auto correlation function (ACF) of the packet loss bitmap.

The main challenge in our mechanism lies in how to guarantee that the packet loss bitmap reported by individual nodes along the route are truthful. Such that reflects the actual status of each packets transmission. Such truthful is essential for correct calculation of the correlation between the loss packets The public auditing problem is constructed based on the (HLA) cryptographic primitives which is basically a signature scheme widely used in cloud

computing and storage system to provide a proof of storage from the server to entrusting clients.

This provides new features such as privacy preserving and low communication channels. In the privacy preserving public auditor should not be able to decern the content of packets delivered on the route through the auditing information submitted by a individual hops, no matter how many independent reports of the auditing information are submitted to the auditor The low communication and storage overheads at intermediate nodes. This makes our mechanism applicable to a wide range of wireless devices, including low cost wireless sensors that have very limited bandwidth and memory capacities.

OBJECTIVE

To estimate the developing a public auditing architecture HLA which ensures to reporting truthful packet on by individual nodes.

A. Existing System

The existing system is a small number of works that differentiate between link errors and malicious packets drops, their detection algorithms usually require the number of maliciously dropping packets to be significantly higher that link errors, in order to achieve an acceptable detection accuracy.

- Depending on how much weight detection algorithm gives to links errors relative to malicious packet drops ,the related works can be classified into the following two categories.
- The first category aims at high malicious dropping rates, where most lost packets are caused by malicious dropping.
- The second category targets the scenario where the number of malicious dropped packets is significantly higher than that caused by link error, but the impact of link error is non-negligible.

B.Proposed System

The proposed system provides the truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function(ACF) of the packets loss bitmap-a bitmap describing the loss/received status of each packet in a sequences of consecutive packets transmissions

- The proposed system with new HLA construction is collusion-proof .
- Construction incurs low communication and storage overheads at intermediate nodes.

  This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to typical storage server scenario, where bandwidth storage is not considered an issue.

- To correctly calculate the correlation between loss packet it is critical to enforce a

  truthful packet loss bitmap reported by each node

- We use HLA cryptographic primitives for this purpose .The basic idea of our method is

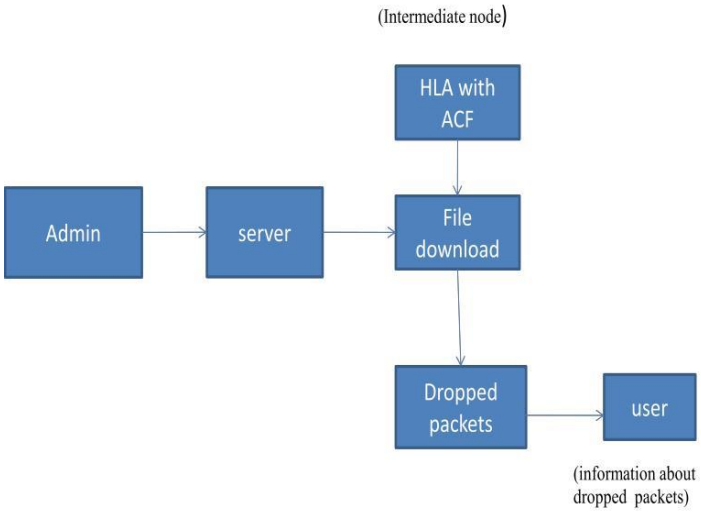
  as follows. An HLA scheme allows the source which has knowledge of the HLA secrete key to generate a HLA signatures.

- The source send outs Ri's and Si's along route. The HLA signatures are used as the

  basic to contract a valid HLA signatures for any arbitrary liner combination of the messages.

III. SYSTEM DESIGN

A.System Architecture



VI. SYSTEM IMPLEMENTATION MODULES:

S and D is truthful, because detecting attacks is in their interest.

- Initiation Phase
- Packet Transmission Phase
- Audit Phase
- Detection Phase

A.INITIATION PHASE

The user have a register and login to access the database. The authorization and authentication facilities the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The admit encrypted the file using RSA and use public key cryptosystem for key distribution and then upload the server. In this phase take place right after route PSD is established but before any data packets are transmitted over the route. The key distribution S also needs to set up its HLA keys.

B. PACKET TRANSMISSION PHASE

A network packet is formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users that if the network were circuit switched.

The signatures are then send together with Pi to the route by using a one way chained encryption that prevents an upstream node. Deciphering the signatures intended for downstream nodes. The database is maintained at every node on PSD.

C. AUDIT PHASE

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, S's HLA public key information, the sequence number of the most recent M packets send by S, and the sequence number of the subset of these M packets that were received by D. Recall that we assume the information send by

D. DETECTION PHASE

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase included the following : detection any overstatement of packet loss at each node, construction a packet-loss bitmap for each hop, calculating the autocorrelation functions for the packets loss on each hop, and deciding whether malicious behavior is present. The above detection process applies to end to end path. The detection for multiple paths can be performed as multiple independent detections, one for each path.

V. CONCLUSION

We shows the comparison with conventional detection algorithm that utilize the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet loss information at individual nodes. so, the author developed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. By this, we can consume the data storage and timing in repeatation of sending files with packet dropping. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in our future works.

VI. FUTURE ENHANCEMENT

From this proposal mechanisms are limited to static or quasi-static wireless ad hoc networks. Frequent changes on topology and link characteristics have not been considered. Extension to highly mobile environment will be studied in our future work. In additional, we have assumed that source and destination are truthful in following the established protocol because delivering packets end to end is in their interest. Misbehaving source and destination will as a proof of concept, we mainly focused on showing the feasibility of the proposed cypto-primitives and how second order statistics of packet loss can be utilized to improve detection accuracy. As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy preserving requirement for the auditing process, and the randomness of wireless channels and packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. This Implementation and optimization of the proposed mechanism under various particular protocols will be considered.

References

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

2.C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610. Fig. 11. Detection accuracy of block-based algorithms.

3.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.

4.B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

5.B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

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

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

8.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.

9.L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

10.J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003.

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

12. W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

13. 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 Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

14.Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

15.D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

16.W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.

17.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.

18.K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement- based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

19.Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in Proc. IEEE WCNC Conf., 2003, pp. 1510–1515.

20.S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom Conf., 2000, pp. 255–265.