International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by

Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

DETECTION OF PACKET DROPPING IN AD HOC NETWORKS

R Reena[1]*, B Hemalatha[1], K Heerajan[1], A Jenifercruz[1], and P Menaka

*Corresponding Author: **R Reena***

The two sources for packet losses in multi-hop wireless ad hoc networks are link error and malicious packet dropping. This paper demonstrates that determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. It is achieved through the implementation of homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads.

Keywords: Packet dropping, Secure routing, Attack detection, Homomorphic linear signature, Auditing

INTRODUCTION

Wireless ADHOC Networks

Ad hoc networks, which are also called mesh networks, are defined by the manner in which the net-work nodes are organized to provide pathways for data to be routed from the user to and from the desired destination. The term mesh network accurately describes the structure of the network: All available nodes are aware of all other nodes within range. The entire collection of nodes is interconnected in many different ways, just as a physical mesh is made of many small connections to create a larger fabric.

Figure 1 provides a simple diagram illustrating these concepts. This diagram is modeled after a wireless "hot spot," where an adhoc network links users to a router with access to the Internet. In this example, two users are highlighted, showing two paths through several nodes to the router.

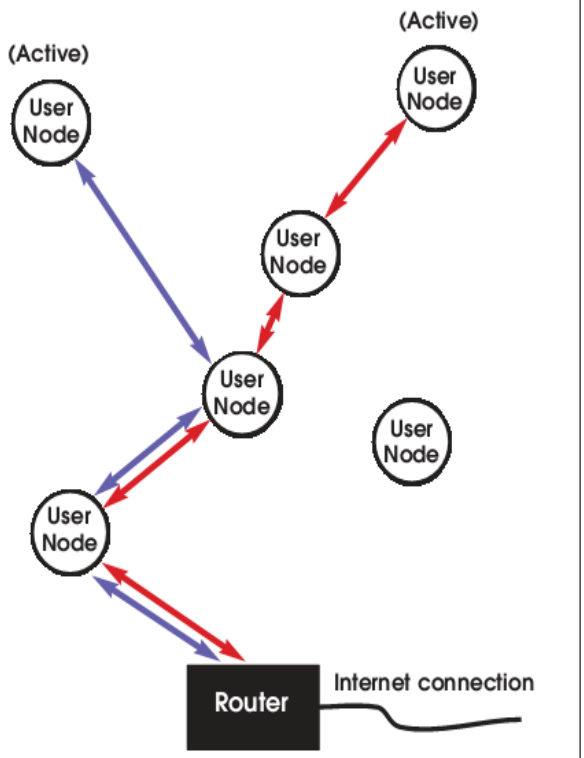
ADVANTAGES OF AD HOC NETWORKS

The principal advantages of an ad hoc network include the following:

- Independence from central network administration
- Self-configuring, nodes are also routers
- Self-healing through continuous re-configuration

[1] VSB Engineering College, CSE.

Figure 1: Basic Structure of an Adhoc, or Mesh, Network



- Scalable—accommodates the addition of more nodes
- Flexible—similar to being able to access the Internet from many different locations

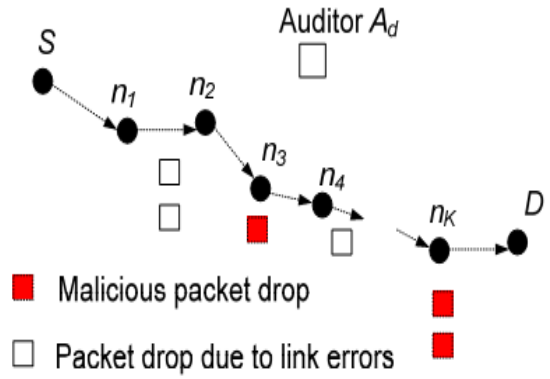
PROBLEM DEFINITION

While ad hoc networks are typically used where they have the greatest emphasis on its advantages, Packet losses are major problem.

In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. Consider an arbitrary path PSD in a multi-hop wireless ad hoc network, as shown in Figure 2. The source node S continuously send packets to the destination node D through intermediate nodes n1,.. . ,nK

In this network, nodes cooperate in relaying/ routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery process. Once being included in a route, the adversary starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination.

Figure 2: Network and attack model



Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet 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 e.g., fading, noise, and interference, link errors, or by the insider attacker. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by

observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss.

LITERATURE SUMMARY

The related work can be classified into the following two categories.

The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories.

The first sub-category is based on credit systems. A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

The second sub-category is based on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route.

The third sub-category of works relies on end-to end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

The fourth sub-category addresses the problem using cryptographic methods. Existing work utilizes Bloom filters to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates.

The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

PROPOSED ALGORITHM

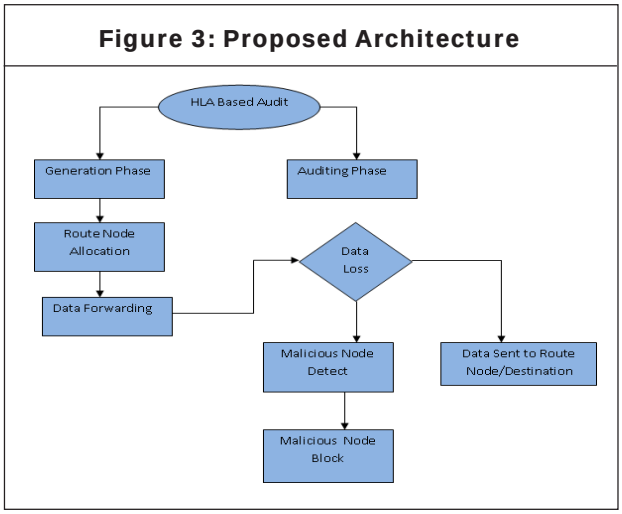
To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.

By detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop. The main challenge in our mechanism lies in how to guarantee that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflect the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets, this can be achieved by some auditing.

Considering that a typical wireless device is resource-constrained, we also require that a user should be able to delegate the burden of auditing and detection to some public server to save its own resources. Public-auditing problem is constructed based on the homomorphic linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients.

Fig 3 shows the Proposed Architecture Scheme. Our detection architecture consists of two phases: Generation Phase, Auditing Phase

Figure 3: Proposed Architecture



GENERATION PHASE

In the evidence generation phase, the nodes will generate contact and data forwarding evidence for each contact or data forwarding. In this process, we define data forwarding evidences that could be used to judge if a node is a malicious one or not. For an investigation target Nj, both of Nj and other nodes will submit their contact history evidence to TA for verification. The nodes with sufficient contact with other users fail to forward the data will be regarded as a malicious or selfish one.

AUDITING PHASE

In the auditing phase, TA will distinguish the normal nodes from the malicious nodes. TA will launch an investigation request toward node Nj in the global network during a certain period. To check if a suspected node Nj is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by Nj.

CONCLUSION

In this paper, we developed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route. To reduce the computation overhead of the baseline construction, a packet block based mechanism was also proposed, which allows one to trade detection accuracy for lower computation complexity.

REFERENCES

1. J N Arauz. 802.11 Markov channel modeling. Ph.D. Dissertation, School of Information Science, University of Pittsburgh, 2004.
2. C Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 598–610, Oct. 2007.
3. G Ateniese, S. Kamara, and J. Katz. Proofs of storage from homo-morphic identification protocols. In Proceedings of the International Conference on the Theory and Application

of Cryptology and Informa-tion Security (ASIACRYPT), 2009.

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 TISSEC, 10(4), 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 Transactions on Information System Security, 10(4):11–35, 2008.
6. K Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: preventing selfishness in mobile ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2005.
7. D Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, Sept. 2004.
8. S Buchegger and J. Y. L. Boudec. Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the ACM MobiHoc Conference, 2002.
9. 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.
10. J Crowcroft, R. Gibbens, F. Kelly, and S. Ostring. Modelling incentives for collaboration in mobile ad hoc networks. In Proceedings of WiOpt, 2003.
11. J Eriksson, M. Faloutsos, and S. Krishnamurthy. Routing amid colluding attackers. 2007.
12. W Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor: Scalable secure routing for ad hoc networks.In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, march 2010.
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 Proceedings of the IEEE ICC Conference, 2009.
14. Q He, D. Wu, and P. Khosla. Sori: a secure and objective reputation-based incentive scheme for ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2004.
15. D B Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172, 2001.
16. W Kozma Jr. and L. Lazos. Dealing with liars: misbehavior identi-fication via Renyi-Ulam games. In Proceedings of the International ICST Conference on Security and Privacy in Communication Networks(SecureComm), 2009.
17. W Kozma Jr. and L. Lazos. REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009.
18. K Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgement-based approach for the detection of routing misbehav-ior in MANETs. IEEE Transactions

on Mobile Computing, 6(5):536–550, May 2006.

19. Y Liu and Y. R. Yang. Reputation propagation and agreement in mobile ad-hoc networks. In Proceedings of the IEEE WCNC Conference, pages 1510–1515, 2003.

20. S Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the ACM MobiCom Conference, pages 255–265, 2000.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com