International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

A PERFORMANCE EVALUATION OF HLA ARCHITECTURE FOR PACKET DROPPING ATTACKS IN WIRELESS AD-HOC NETWORK USING NS2

Dr. T. Ramaprabha,
Professor,
Department of Computer Science & Applications1
Vivekanandha College of Arts and Sciences for Women
(Autonomous), Namakkal,
TamilNadu, India.

M.Karthika,
M.Phil Research Scholar,
Department of Computer Science & Applications[2]
Vivekanandha College of Arts and Sciences for Women
(Autonomous), Namakkal,
TamilNadu, India.

Abstract: Link error and malicious packet dropping are two sources for packet losses in wireless ad hoc network. While observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious packet 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 lost packets. In this paper, we develop a 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 construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed. In this paper, we improve the performance and good delivery ratio like throughput ratio, end to end delay ratio and Packet loss ratio in over wireless Adhoc network.

Keywords: Wireless Ad-hoc Network (WANET), Packet dropping, secure routing, attack detection, Homomorphic Linear Authenticator (HLA), public auditing.

I. INTRODUCTION

In the absence of a supporting infrastructure, wireless ad hoc networks realize end -to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. Moreover, selfish nodes may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is known as node misbehavior. Existing solutions for identifying misbehaving nodes either use some form of per-packet evaluation of peer behavior. On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing or achieving of Per-packet acknowledgement. This type of monitoring operations must be repeated on every hop of a Multihop route, thus it requires high communication overhead and energy expenditure. Also, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected. Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes and reputation values are given to node according to its functionality of packet forwarding.

Wireless Network: Wireless network technologies come in several forms such as wireless PAN, Wireless LAN and Wireless WAN. These networks have their own characteristics and properties. Wireless PANs are those networks in which the interconnected devices communicate using either Zig Bee or Bluetooth.

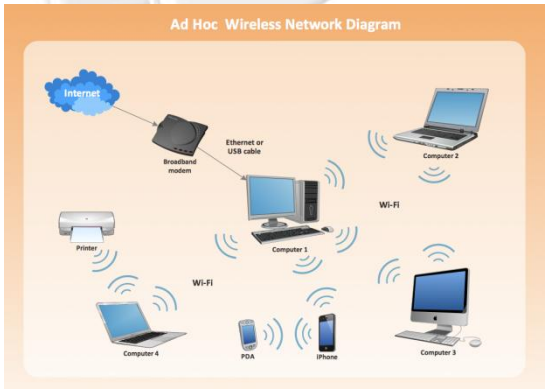

Figure 1: Wireless adhoc network

The range of this communication is very less, say 10m.Wireless LANs are networks that have various devices capable of communicating with each other.

Adhoc- Network

An ad-hoc network can be formed when a group of mobile devices communicate with each other without depending on any fixed infrastructure. In such cases, neighbouring nodes communicate with each other while the communication between non-neighbour nodes is performed via the

intermediate nodes that can act as routers. The network topology frequently changes in the adhoc network. Ad-hoc wireless network are prone to route breaks due to various sources such as node mobility, signal interference, high error rate and packet collision.

Routing in Adhoc Network: Routing in an adhoc network is the most important task that needs to be handled with care. Since the nodes in an adhoc network depend on intermediate nodes, for carrying the data there are various routing protocols used in this process. The main aim of routing protocols in an adhoc network is to find minimum hop distance between the source and destination with minimum overhead and bandwidth. Depending on the routing topology, they are classified as proactive, reactive and hybrid.

II. PROPOSED WORK MODEL USING HLA

In this paper, we develop an accurate algorithm for detecting selective packet drops made by insider attackers. Our 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. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, 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. Our algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

Merits of Proposed System in HLA

- The proposed system with new HLA (Homomorphic Linear Authenticator) construction is collusion-proof.
- The proposed system gives the advantage of privacy-preserving.
- Our 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 the typical storage-server scenario, where bandwidth/storage is not considered an issue.
- Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

III. ROUTING SYSTEM ARCHITECTURE

In this paper, we focus on the privacy issue, i.e., how to prevent traffic analysis/flow tracing and achieve source anonymity in MWNs. Among all privacy properties, source anonymity is of special interest in MWNs. Source anonymity refers to communicating through a network without revealing the identity or location of source nodes. Preventing traffic analysis/flow tracing and provisioning source anonymity are critical for privacy aware MWNs, such as wireless sensor or tactical networks. Consider a simple example of multicast communication in military ad hoc networks, where nodes can communicate with each other through multi-hop packet forwarding.

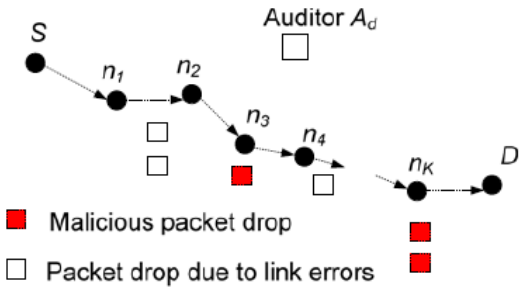

Figure 2: Routing System architecture

If an attacker can intercept packets and trace back to the source through traffic analysis, it may disclose some sensitive information such as the location of critical nodes (e.g., the commanders) and then further it may impair the location privacy. Subsequently, the attacker can take a series of actions to launch the so called Decapitation Strike to destroy these critical nodes. Another example is the event reporting in wireless sensor networks, where flow tracing can help attackers to identify the location of concerned events, e.g., the appearance of an endangered animal in a monitored area, and then take subsequent actions to capture or kill the animals.

V. EXPERIMENTS AND RESULTS

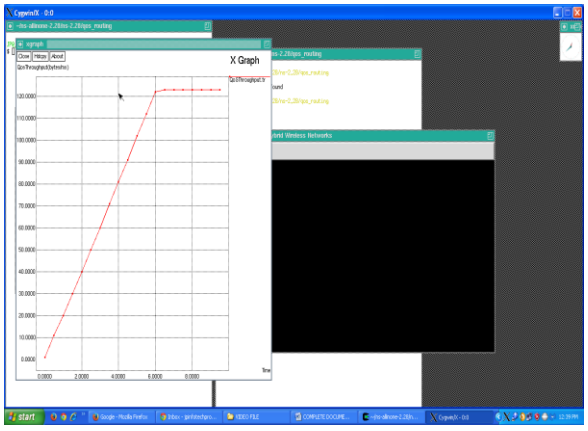

Figure 3: Throughput Ratio

Throughput: is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.

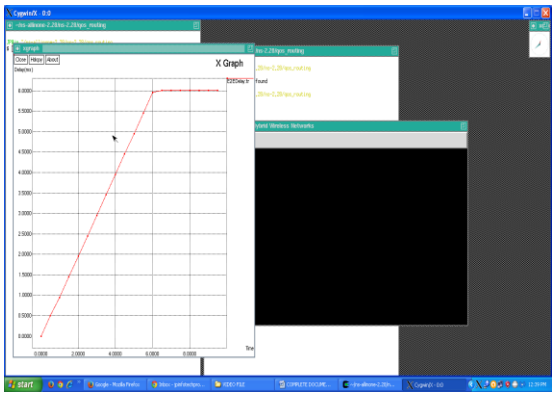

Figure 4: End to End Delay Ratio

End to End latency: It refers to the time taken for a packet to be transmitted across a network from source to destination. These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the X graph to get graph as the output.

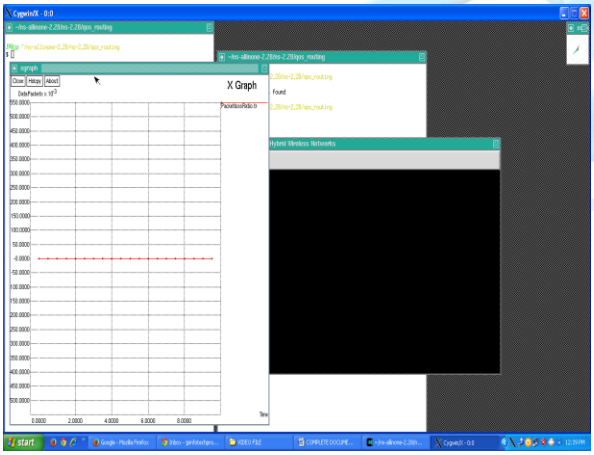

Figure 5: Packet loss Ratio

Packet loss ratio: measures the ratio of packets have been dropped during transmission time

IV. CONCLUSION

In this paper correlations of lost packet are correctly calculated. To ensure the truthfulness of information send by the nodes HLA based auditing architecture is used to provide privacy preserving collision avoidance and low communication storage overheads. Extension to dynamic environments will be studied in our future work.

V. REFERENCES

[1]. A. Broch, Marwan Krunz," Detection of Malicious Packet Dropping in Wireless Ad HocNetworks Based on Privacy-Preserving Public Auditing" in Proc. IEEE Int. Conf. Netw. Protocols vol. 8, no. 5, pp. 579–592, Oct. 2003

[2]. A. Johnson, D. A. Maltz, , "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.

[3]. B. 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, AdHoc Wireless Netw., Sophia Antipolis, France, 2003.

[4]. C.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]. C.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.

[6]. 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.

[7]. D. 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.

[8]. D. 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.

[9]. D. Xue and K. Nahrstedt, "Providing fault-tolerant ad-hoc routing service in adversarial environments," Wireless Pers. Commun., Special Issue Secur. Next Generation Commun., vol. 29, no. 3, pp. 367–388, 2004.

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

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

[12]. 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.

[13]. W. Buttyan and J. P. Hubaux, "Stimulating cooperation in self organizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.