International Journal on Applications in Engineering and Technology
Volume 2: Issue 4: April 2016, pp 4-7. www.aetsjournal.com ISSN (Online) : : 2455-0523

Privacy Conserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks

DurgaN, Philem Sofia Devi, Soniya K Jose, SwethaSasidharan, Mrs.L.Thenmozhi,

Abstract— An Ad-hoc network is a wireless network formed by wireless nodes without any help of infrastructure. Link error and malicious packet dropping remains as the two sources for packet losses in wireless Ad-hoc network. The packet loss rate were detected and the truthfulness of this packet-loss information were achieved using DSR(Dynamic Source Routing). Based on HLA (HomomorphicLinear Authenticator), a public auditing architecture was developed to allow the detector to verify the truthfulness of the packet loss information. This construction is privacy preserving, incurs low communication and storing overheads holding good only for smaller networks. So a construction is proposed using EGMP (Efficient Geographical Multicasting Protocol), for larger networks to divide into zones. The challenge is the difficulty to detect the place (or hop) where the packet is dropped but also identifying whether it is intentional or unintentional. For this an accurate algorithm for detecting selective packet drops made by insider attackers is proposed, providing the truthful and decision statistics which can be publicly verified, as a proof to support the detection decision. The high detection accuracy is achieved when the correlations between the positions of lost packets are exploited, as calculated from the auto-correlation function (ACF) of the packet-loss and its status. Truthfulness is essential to calculate the correlation between lost packets correctly. An auditing mechanism is employed allowing auditing of the nodes and all the information associated in the routing of the packets and the nodes in the network.

Index terms: packet dropping, auditing, auto-correlation, multicasting

I. INTRODUCTION

Ad hoc networks, which are also called mesh networks, are defined by the manner in which the network nodes are organized to provide pathways for data to be routed from the user to and from the desired destination. Actually, the two names ascribed to these networks provide considerable insight. Ad hoc has two definitions—the first can be either "impromptu" or "using what is on hand," while the other is "for one specific purpose." For example, members of an ad hoc committee (studying a specific issue) might discover that they are attending the same event and decide to have an ad hoc (impromptu) meeting. Ad hoc networks follow both definitions, as well. They are formed as they are needed (impromptu), using resources on hand, and are configured to handle exactly what is needed by each user—a series of "one specific purpose" tasks. 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. An ad hoc network links users to a router with access to the Internet.

If one of the intermediate nodes were to fail (e.g. that user leaves the area), the network will automatically reconfigure itself, locating an alternate path from the user to the router. Typically, all available nodes are also network users, each sharing the total data transfer capacity of the particular hardware and operating protocol being used. The network could also connect users to other users directly, as would be done in an industrial control and monitoring network. Since there is no need for central administration of the network configuration, it is most efficient to design the system for autonomous operation of each node. In an industrial environment, a situation such as an alarm would be propagated through the network and received directly by each node. Each node would be programmed to respond according to its particular function—machine control, process monitoring, supervisory personnel or central office.Each node identifies the nodes that are available for communications, based on signal strength, which is mainly related to distance, but is also affected by obstructions or interference. Some nodes may be beyond range, others may be detectable but have insufficient signal strength for reliable communications. Once the available nodes are identified, this information is communicated to other nodes, along with information about the desired destination. Using the lists of available connections, the network configuration algorithm selects a particular routing for each user to its destination. This process requires system operating software to have good decision-making algorithms, based on practical criteria for signal strength, path reliability over time and network configuration patterns.

II. RELATED WORK

Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories. The first aiming at high malicious dropping rates, where most (or

DurgaN, Philem Sofia Devi, Soniya K Jose, SwethaSasidharan, Final Year CSE, Nehru Institute Of Technology, Coimbatore.
Mrs.L.Thenmozhi, Assistant professor, Department of Computer science and Engineering, Nehru Institute of Technology, Coimbatore

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 malicious 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 neighbours to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbours. 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 acknowledgement to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route. The fourth subcategory addresses the problem using cryptographic methods. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. The first hop where the packet is no longer forwarded is considered a suspect for misbehaving. 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. Certain knowledge of the wireless channel is necessary in this case. The traffic were at the MAC layer of the source node according to a certain statistical distribution[7], so that intermediate nodes are able to estimate the rate of received traffic by sampling the packet arrival times. By comparing the source traffic rate with the estimated received rate, the detection algorithm decides whether the discrepancy in rates, if any, is within a reasonable range such that the difference can be considered as being caused by normal channel impairments only, or caused by malicious dropping, otherwise. The malicious packet dropping were detected by counting the number of lost packets in [1],[13]. If the number of lost packets is significantly larger than the expected packet loss rate made by link errors, then with high probability a malicious node is contributing to packet losses. All methods mentioned above do not perform well when malicious packet dropping is highly selective. More specifically, for the credit-system-based method, a malicious node may still receive enough credits by forwarding most of the packets it receives from upstream nodes. Similarly, in the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop. While the Bloom-filter scheme is able to provide a packet forwarding proof, the correctness of the proof is probabilistic and it may contain errors. For highly selectively attacks (low packet-dropping rate), the intrinsic error rate of Bloom filer significantly undermines its detection accuracy. As for the acknowledgement-based method and all the mechanisms in the second category, merely counting the number of lost packets does not give a sufficient ground to detect the real culprit that is causing packet loss. This is because the difference in the number of lost packets between the link-error-only case and the link-error-plus-malicious-dropping case is small when the attacker drops only a few packets. Consequently, the detection accuracy of these algorithms deteriorates when malicious drops become highly selective. The target proposed here is the challenging situation where link errors and malicious dropping lead to comparable packet loss rates. The effort in the literature on this problem has been quite preliminary, and there is a few related works. Note that the cryptographic methods were used [8] to counter selective packet jamming target a different issue than the detection problem studied in this paper. The methods delay a jammer[8] from recognizing the significance of a packet after the packet has been successfully transmitted, so that there is no time for the jammer to conduct jamming based on the content/importance of the packet. Instead of trying to detect any malicious behaviour, the approach is proactive[8], and hence incurs overheads regardless of the presence or absence of attackers.

III. EXISTING SYSTEM

In the previous work, HLA is used to identify the packet loss which at the same time acted as auditor to get the ACK from the nodes and the destination node as well. The truthfulness of the lost packets in the whole network were verified. DSR algorithm was employed for the source routing purposes and to detect the malicious nodes and the distance vector of the nodes.

DISADVANTAGES

- Time consumption by the nodes is high
- Holds good only in small networks
- Status of the nodes being good or bad is not maintained

IV. PROPOSED SYSTEM

A larger network is considered, the network is splitted up into zones using EGMP algorithm. Each and every sub zones contains a header containing all the informations of every nodes in its zone. The HLA is still used for the same purpose as it has in the existing system. DSR and Receiver based algorithm is used to detect the malicious nodes and the acknowledgements from the receiver.

ADVANTAGES

- Time consumption by the nodes is reduced
- Holds good for both large and small network
- Packet delivery is efficient compared to the existing system.
- Status of the nodes being good or bad is maintained

SYSTEM DESIGN

Input design

Input design is the process of converting user-originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system.

The input design is made in various NAM forms with various methods.

- Node creation
- Protocol Implementation
- Simulation results

Output design

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application. In any system, the output design determines the input to be given to the application.

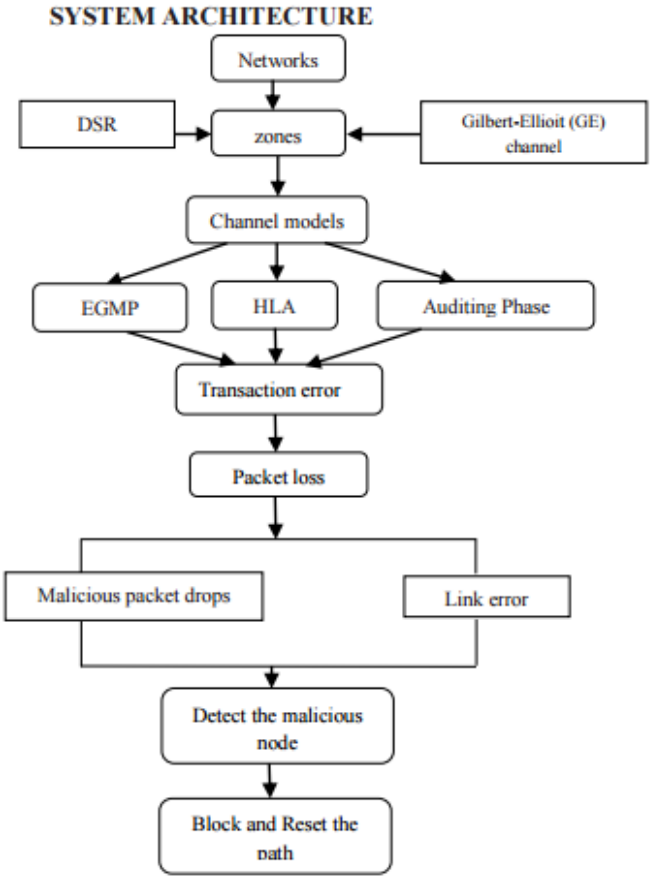


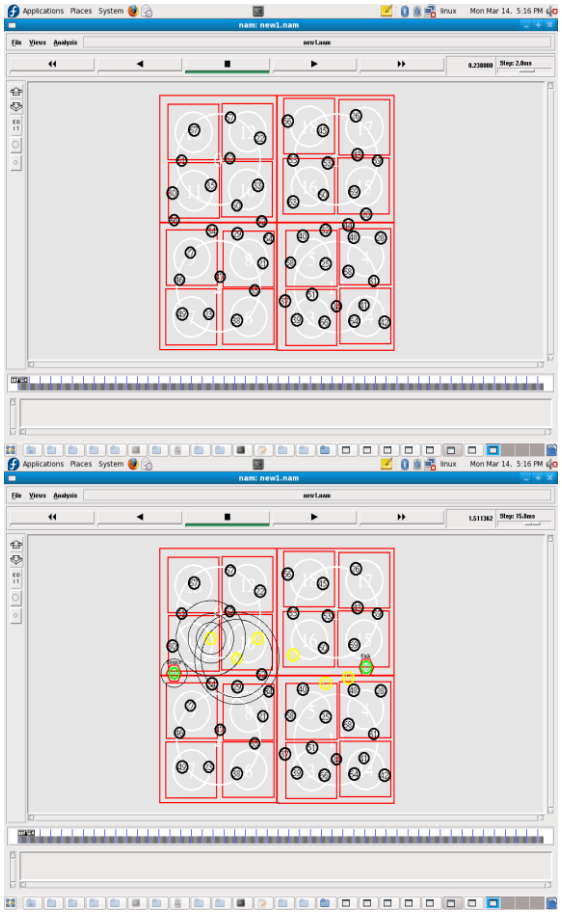
Fig no.1:System Architecture

LIST OF MODULES

- System authentication
- Attacker detection
- Attacker aware traffic allocation

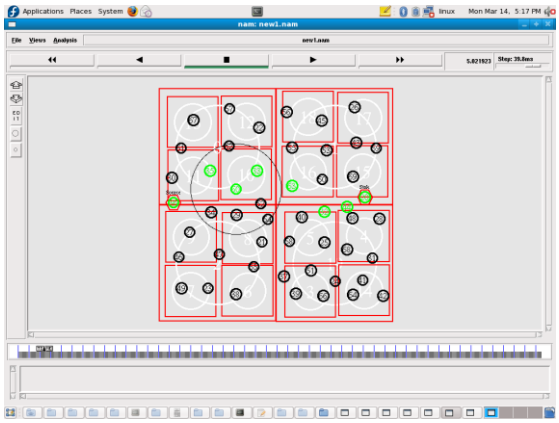
SYSTEM AUTHENTICATION

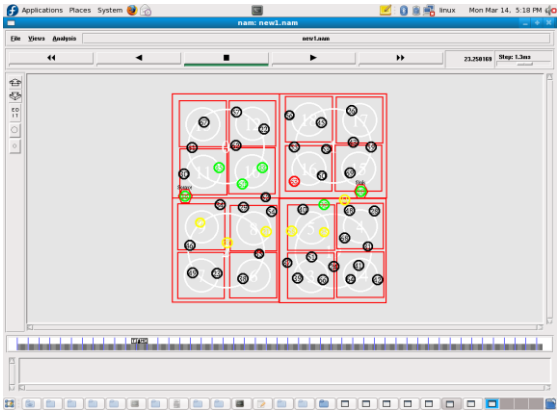
Initially the network is established and the nodes are distributed in the divided zones. The source and destination nodes is assigned as per desired. The packet size to be sent is checked. Possible paths for the packets to be sent are found out.



ATTACKER DETECTION

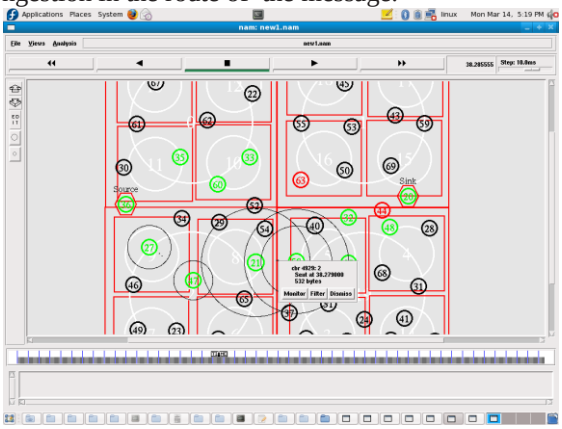
In this the possible causes of the packet loss are detected. An empty message is established between the source and destination. If it is found to be attacked then the detection starts here.The attacks caused by malicious nodes are detected and the location of those nodes are detected.





ATTACKER AWARE TRAFFIC ALLOCATION

In this process the detected nodes are studied of the traffic it associates. Once it is done then the nodes are deleted to reduce the traffic allocation, size of the network and reduce congestion in the route of the message.



V.CONCLUSION

The correlation between lost packets are exploited significantly improving the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To correctly calculate the correlation between lost packets truthful packet-loss information at individual nodes is acquired. An HLA-based public auditing architecture is developed ensuring truthful packet-loss reporting by individual nodes which proves to be collusion proof. The cause of the packet loss is detected and the malicious nodes. To reduce the computation overhead of the baseline construction, a packet-block-based mechanism is also used and the detected malicious nodes are deleted. The efficiency of the implementation are proved compared with the existing implementation based on throughput, packet drops, packet delivery and energy consumption by the nodes in the network.

VI. FUTURE WORK

Link error sinks mobility to prolong the network lifetime in networks where the information delay caused by moving the sink should be bounded. Due to the combinational complexity of this problem, most of the proposals focus on homomorphic and the detection algorithms remains unknown. Can be enhanced building a unified framework for analysing this joint sink mobility, routing, delay, and so on. The induced sub-problems and present efficient solutions for them can further be discussed. The solutions found can be generalized and a polynomial-time optimal algorithm may be proposed for the origin problem. The effects of different trajectories of the sink and important insights for designing mobility schemes can be provided in real-world mobile network. Misbehaving source and destination will be pursued in our future research.

REFERENCES

[1] Abhishek Jena, RameswariBiswal, ThiyamRomila Devi, Vikram Kumar, Nov-2013,"Implementation of Dynamic Source Routing(DSR) in mobile Ad-hoc Netwrok(MANET)",IJRET: International Journal of Research in Engineering and Technology -ISSN: 2319-1363 | ISSN: 2321-7308,Volume: 02 Issue: 13

[2] G. Anandhi, S. K. Srivatsa,(2012),"Joining Delay, Packet Delivery and Limitations of EGMP",International Journal of Science and Research (IJSR)-ISSN (Online): 2319-7064,Volume 3 Issue 1

[3] Amit Kumar Sanghi,Dr. Dharm Singh, RakeshPoonia, February 2013 ,"DSR Routing Protocol in Wireless Ad-hoc Networks: Drop Analysis" ,International Journal of Computer Applications (0971 – 8887) Volume 14– No.7,

[4] Mrs. R.Bamalakshmi, Karthick P N, December-2013,"Detecting malicious packet dropping and secure trace out in wireless Ad-hoc Network",International Journal For Technological Research In Engineering Volume 3, Issue 4

[5] T. Hayajneh, T. Kim, P. Krishnamurthy and D. Tipper, "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.

[6] Kennedy Edemacu, Martin Eukuand Richard Ssekibuule, September 2014 ,"Packet drop attack detection techniques in wireless Ad-hoc Networkss:A review" ,International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1

[7] G. Kesidis and R. Rao, "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. 2917–2961.

[8] L. Lazos and A. Proano, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.

[9] Marwan Krunz, Tao Shu, Fellow, IEEE, APRIL 2013 ,"Privacy Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad-Hoc Networks",IEEETransactions on Mobile Computing , Vol. 14, No. 4

[10] Noble George, Sujitha M, July 2013 ,"Truthful Detection of Packet Dropping Attack in MANET ",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7

[11] G Sadashivappa,SridharaHansanoor, (June 2012),"A New Energy Efficient and Scalable Multicasting Algorithm for Hierarchical Networks",International Journal of Engineering Research and Development- ISSN: 2278-067X, Volume 1, Issue 1

[12] Saranya.S, P.D.R. Vijayakumar,July 2014 ,"An Efficient Genetic Approach Based Geocasting Protocol for Video Streaming in MANET" ,International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Special Issue.

[13] W. Trappe, T. Wood, W. Xu and Y. Zhang, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM MobiHoc Conf., 2001, pp. 46–17.