CEM: CRITICAL EVENT MONITORING FOR HOMOMORPHIC LINEAR AUTHENTICATOR IN PACKET DROPPING ATTACKS

Riyad A M, Assistant Professor of Computer Science, EMEA College of Arts & Science, Kondotty, Malappuram(dist.), Kerala

Abstract:

While observing a series of packet losses in the network, critical event monitoring in the network, just a small number of packets need to be sent most of the time. When a crucial event happens, an alert should be sent to the whole network. Some sleep scheduling techniques are constantly used in networks, causing considerable transmission latency, particularly in big networks. A new sleep scheduling technique has to minimize network for alarm broadcasting latency. Design two traffic routes for the delivery of alarm message based wake-up pattern. The insider-attack scenario, where hostile nodes use their knowledge of the communication environment to choose discard a tiny number of packets essential to the network performance, is of particular interest. Because the packet loss rate is similar to the channel error rate, traditional algorithms cannot achieve acceptable detection accuracy. This paper proposed Critical Event Monitoring (CEM) using correlations between missing packets to enhance detection accuracy. Also, to guarantee accurate connections, Develop a public auditing architecture based on homomorphic linear authenticators (HLA) that enables the detector to validate node packet loss information. This design protects privacy, prevents collusion, and saves on communication and storage costs. A packet-block-based method is also suggested to decrease the baseline scheme's processing cost. This paper shows that the suggested mechanisms outperform traditional techniques like maximum-likelihood detection in extended simulations.

Keywords: HLA, CEM, Packet dropping, DoS, Evidence Node

I INTRODUCTION

Nodes in a multi-hop wireless network work together to relay/route data. An enemy may take advantage of this cooperative nature to conduct attacks [1]. For example, the adversary might appear to be a cooperative node in the route discovery process at initially. After being added to a route, the adversary begins discarding packets [5]. In its most extreme version, the rogue node simply ceases forwarding all packets received from upstream nodes, totally interrupting the link between the source and the destination. A strong denial-of-service (DoS) assault may eventually cripple the network by splitting its topology. Even while continuous packet dropping may substantially impair network speed, such an “always-on” assault has drawbacks from the attacker's perspective. For starters, the persistent existence of very high packet loss rates at the malicious nodes makes this kind of assault easily detectable. Second, once discovered, these attacks are simple to counter [6]. For example, if an attack

is discovered but the malicious nodes are not identified, the randomized multi-path routing methods may be used to avoid the black holes created by the assault, thus probabilistically removing the attacker's danger. If the malicious nodes are also discovered, the risks posed by these nodes may be fully removed by removing them from the network's routing table [7].

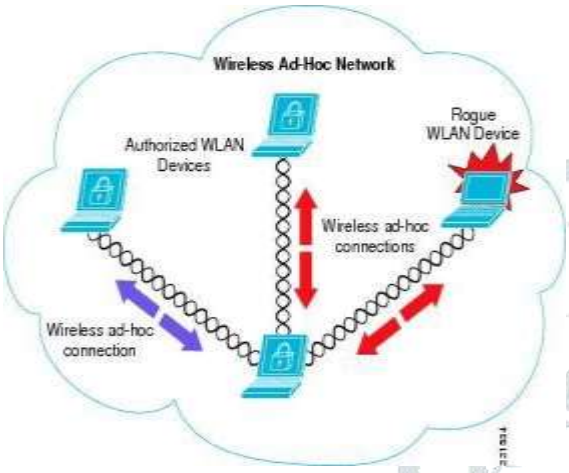

Figure 1: Wireless Ad-hoc Network Architecture

A malicious node on the route may use its knowledge of the network protocol and the communication environment to conduct an insider attack, which can accomplish the same performance degradation impact as a persistent assault at a considerably lower chance of detection. In particular, the rogue node may assess the significance of different packets and then discard the tiny number considered extremely essential to network functioning [8]. In a frequency-hopping network, for example, these could be packets that convey frequency hopping sequences for network-wide frequency-hopping synchronization in an ad hoc cognitive radio network; or they could be packets that carry idle channel lists (i.e., whitespaces) used to establish a network wide control channel. The authors of have shown that an occasional insider attacker may inflict substantial network damage with a low chance of being detected by targeting these extremely important packets. This paper is interested in countering such an insider assault in this article. This paper is particularly interested in the issue of detecting and identifying the malicious node(s) responsible for selective packet drops [9]. Detecting selective packet-dropping attacks in a highly dynamic wireless environment is very difficult. The challenge stems from the need that this paper not only detect the location (or hop) where the packet is lost, but also determine whether the drop was deliberate or accidental [10]. Because of the open nature of the wireless medium, a packet loss in the network may be caused by severe channel conditions (e.g., fading, noise, and interference, often known as link faults) or by an insider attacker. Link failures are very substantial in an open wireless setting, and may not be much lower than the insider attacker's packet dropping rate [11] [12]. As a result, the insider attacker may blend in with the severe channel circumstances. In this instance, just monitoring the packet loss rate is insufficient to pinpoint the precise source of a packet loss. The aforementioned issue has received little attention in the literature [13].

II BACKGROUND STUDY

Tao Shu and Marwan Krunz suggested in their work that nodes cooperate in transmitting or routing activity in a multi-hop system [1]. An opponent may take advantage of this nice nature to launch attacks. As an example, the adversary may first claim to be the pleasant node in the route building process. The adversary begins dropping packets as soon as he is incorporated into a

strategy. While in the majority of severe structure, the malicious node basically stops providing every supply obtained from upstream nodes, completely disrupting the path between the foundation and the objective. Finally, such severe Denial-of-Service (DoS) damage may be mitigated simply by dividing its topology. Despite the fact that persistent supply decline may effectively degrade the overall performance of the multi-level, from the attacker's perspective, this kind of "typically for" damage has its own benefit. For starters, the malicious node's continuous greater supply decrease quantity makes this kind of damage extremely easy to identify. Second, once recognized, these methods are generally simple to alleviate. A couple of reasons causing supply reduction in the multi-hop Wi-Fi ad-hoc network are website connection error and malicious supply dropping. With determining whether the failures are caused only by a website link error or by the combined impact of a website link error and a malicious drop. Were particularly motivated by the fundamental assault scenario, in which malicious nodes that may be a part of the training misuse their unique specifics with the communicating framework specifically drop a little degree of packages required for multilevel execution. Because the supply declining amount for this situation is comparable to the funnel error amount, conventional information generated from particular the supply declining amount may achieve pleasant recognition accuracy.

In their paper, Eugene Y. Vasserman and Nicholas Hopper suggested that [2], the wireless Ad-hoc sensor organizes and routes information in them to particular attackers. As a result, this paper must ensure a reliable and verified information transfer method. There are many methods created to protect against a DOS attack; nevertheless, it is not completely feasible. The Vampire attack, which drains node life from the wireless ad hoc sensor network, is one such DOS assault. This article examines resource use bursts on the course plotting standard protocol covering, which will always impede system by simply quickly assets node battery level. These "Vampire attack" attacks will not be specific to any one standard protocol, but will instead vary based on the characteristics of many common classes of course-plotting protocols. Most individuals consider methods to rationalize these types of attacks, including one additional proof-of-concept that may limit the damage caused by Vampires during your packet sending stage.

Wenyuam XU, Yanyoung Zhang, and Timothy Wood presented a study that evaluates radio barrier attacks from both perspectives [3]. In this article, a novel technique for combating reactive jamming attacks is proposed by identifying certain trigger nodes, the activation of which activates reactive jammers. As a consequence, several methods for identifying jamming attacks are discussed in this article, and emphasis is placed on locating reactive jammers. A more effective method is still suggested, which detects and blocks reactive jammers across the Wi-Fi alarm system using the realizing induce nodes.

Routing, as suggested by G. Acs, L. Buttyan, and I. Vajda, is a standout among the most fundamental networking functions in mobile ad hoc networks [4]. They devised a specific

composition in which stability can be simply specified and routing networks for mobile ad hoc networks may be shown to be secure in a rigorous way. Their specific composition will be aimed towards on-demand supply routing networks, but the general principles are applicable to other types of networks as well. Their approach will be a good simulator paradigm that is already used attentively to the study of important establishing networks, but, to the best of their knowledge, it isn't used for ad hoc routing yet. Furthermore, they offer a new on-demand routing protocol called as endairA, and they demonstrate the use of their composition by demonstrating that it is safe in their model.

A. Proano and L.Lazos presented work that investigates the problem of the attacker or jammer using his inside data for the purpose of conducting specific jamming attacks in which certain messages of high importance are targeted [5]. Throughout this report, the work of fiction approach comprises of reactive jamming episodes by determining the induce nodes, where transmission initializes any kind of reactive jammer. As a result, in this study, a range of methods for detecting jamming damage have been discussed, with a focus on identifying reactive jammers. A strong strategy has been developed that detects and defends reactive jammers over mobile ad hoc networks by using sensing induce nodes.

a) PROBLEM STATEMENT

Diagnosis of distributed packet-dropping attacks is usually challenging in a very dynamic setting. The real solidity may be in such a state that this paper must not only identify the actual position to packet loss, but also determine whether the loss is deliberate or accidental. Precisely, because of the openness associated with wireless origin, the real packet loss inside the community may be caused by severe channel circumstances or by an insider attacker. In a wide-open wireless environment, connection failures are common and will wind up being far lower than the real package dropping rate by the insider attacker. The real discovery must be performed by a public auditor who is unaware of the information utilized by the nodes along the network path. When a malicious node is discovered, the auditor will be able to construct any proof of the node's real harmful conduct.

III CEM SYSTEM MODEL

The fundamental concept behind detecting correlations between lost packets across each hop of the route is to represent the packet loss process of a hop as a random process cycling between 0 (loss) and 1 (gain) (no loss). Consider a series of M packets that are sent sequentially over a wireless channel. The receiver of the hop gets a bitmap by monitoring whether or not the broadcasts are successful. Individual node packet-loss bitmaps provided along the route are accurate, i.e., they represent the real state of each packet transmission. Such honesty is required for accurate assessment of the correlation between lost packets. This is a difficult issue since it is natural for an attacker to submit misleading information to the detection algorithm in order to escape detection. The auto-correlation function of this bitmap is used to compute the correlation of the lost packet. The instantiations of the packet-loss random process should exhibit unique dropping patterns under various packet dropping circumstances, i.e., link-error vs. malicious

dropping (represented by the correlation of the instance). This is true even if the packet loss rate in each instantiation is the same. Shape the traffic at the source node's MAC layer according to a statistical distribution, such that intermediate nodes can estimate the rate of incoming traffic by sampling packet arrival timings. By comparing the source traffic rate to the estimated received rate, the detection algorithm determines if the rate difference, if any, is within an acceptable range such that the difference may be attributed to normal channel impairments alone, or to intentional dropping. Sleep patterns for event monitoring have been developed, with the majority of them focusing on reducing energy usage. Actually, most of the time in critical event monitoring, just a limited number of packets must be sent. When a critical event occurs, the alarm packet should be sent to the whole network as quickly as feasible. As a result, broadcasting delay is a significant problem for the critical event monitoring application. Nodes in a network are often equipped with passive event detection capabilities, which enable a node to notice an event even while its wireless communication module is in sleep mode. When the node detects an incident, the radio module of the node is instantly woken up and ready to deliver an alert message.

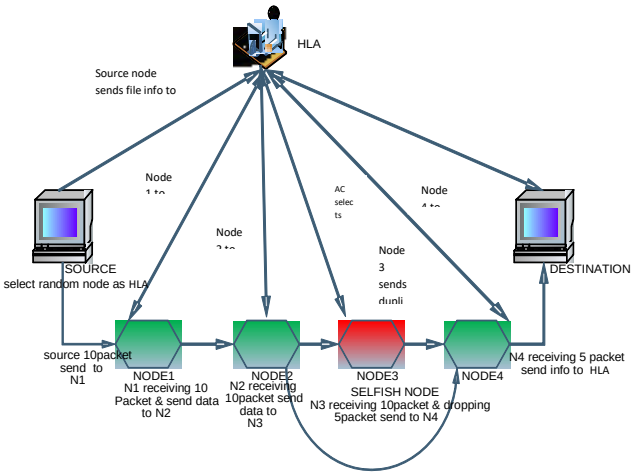

Figure 2: CEM Architecture

a) DATA CENTER

This module's primary purpose is to transmit data between the server and the receiver. Message delivery to the final destination or intermediate nodes. This module is the initiator of data transmission between network communication nodes.

b) HOMOMORPHIC LINEAR AUTHENTICATOR (HLA)

In this module, a node is required to maintain a few signed contact records of its past contacts, which the next contacted node may use to determine if the node lost any packets. Because misbehaving nodes may misreport their contact records in order to escape detection, a tiny portion of each contact record is sent to a set number of evidence nodes, which may gather relevant contact data and identify misbehaving nodes.

To verify the receipts, the HLA must do a significant number of cryptographic operations, which may need unrealistic computing capacity and make practical implementation of these systems complicated or inefficient. Furthermore, since the value of a transaction (relaying packets) may be extremely little, the transaction's cost in

terms of submitting and clearing receipts should be considerably less than its value. As a result, minimizing communication and processing overhead is critical for the successful implementation of alternative route discovery in order to prevent establishing a bottleneck at the HLA and depleting the nodes' resources.

c) FORWARDING NODE

The data is transferred between the server and the receiver through the forwarding modules. The routing is built before the data forwarding mechanism to execute the forwarding mechanism. Once the data has been sent, an acknowledgment of the data transfer information will be provided to the accounting centre.

d) PACKET DROPPING & DETECTION

To solve the issue, this paper presents a distributed system to identify packet dropping in Distributed networks, as well as a method to restrict bandwidth flowing to misbehaving nodes. First, this paper present a method for detecting packet drops in a distributed way. In this method, a node must retain prior signed contact records, such as buffered packets and packets transmitted or received, and send them to the next HLA, which may determine whether the node reduced block size based on the provided data.

e) EVIDENCE NODE

Evidence is being sought in order to detect and evict cheating nodes that provide false reports. Instead of seeking Evidences from all nodes involved in the cheating reports,

To identify misreporting, the contacted node additionally randomly chooses a specific number of evidence nodes for the reported records and contacts them with a summary of each reported record. The evidence node may identify the misreporting node if it gathers two conflicting contact records. To identify misreporting, a normal node chooses evidence nodes and sends the record summary to them for each contact record that it creates with (or gets from) other nodes. The summary only contains a portion of the data required to identify inconsistencies caused by misreporting. Following the evidence node information, the AODV protocol determines an alternative route and delivers a block of packets to the target. The destination is built securely to accept a block of packets from the forwarding node.

f) Algorithm step:

Step 1: initializing the packet rate

Step 2: initializing available of packet rate.

Step 3: initializing detection accuracy

Step 4: initializing and calculate link errors rate

Step 5: initializing route

Step 7: Checking packet rate each route

Step 8: Calculating for detection accuracy in each route

Step 9: Calculating selects detection accuracy

Step 10: Calculating marginal supply

Step 11: Calculating receiving packet rate

Step 12: Calculating for update packet rate

Step 13: Calculating for route node accuracy

g: Algorithm:

Find packet rate indicative node p^* using

Find available of packet rate in node;

Collect data detection accuracy;

Calculate link errors and malicious drop using

Select a set of route

$$P'_x = \{y \mid \rho_{xy} \geq \rho_{\min},\ \gamma_{xy} \geq \gamma_{\min},\ \tau_a \geq \tau a_{\min}\};$$

order the route of set P'_x according to detection accuracy utility function: $P_x=\{u_{xj} \geq \cdots \geq u_{xi} \geq \ldots\}$;

form P'_x by taking the first L nodes from P_x;

for each $y \in P_x$ form a set of route P_y selects detection accuracy y;

each detection accuracy y calculates its marginal demand function as $\Sigma x \in py\ D_{bx}$;

each route x calculates its marginal supply function as $\Sigma y \in P_x\ S_{by}$;

$y \leftarrow 0$;

repeat

$y \leftarrow y + 1$; $t \leftarrow 0$; $p_{xy}(t) = p^*$;

Calculate learning rate σ_y;

Calculate price $p_{xy}(t + 1)$;

while $|p_{xy}(t + 1) - p_{xy}(t)| > \varepsilon$ do

Demand and supply are updated

$t \leftarrow t + 1$;

Calculate packet rate σ_y;

Update packet $p_{xy}(t + 1)$;

end while

until $y \leq L$

Select sending detection accuracy y at route p^*_{xy};

Calculate route own experience using and update recommender's trustworthiness using.

IV RESULTS AND DISCUSSION

The proposed model has implemented by using C#.net programming language. The results are verified with Event monitoring.

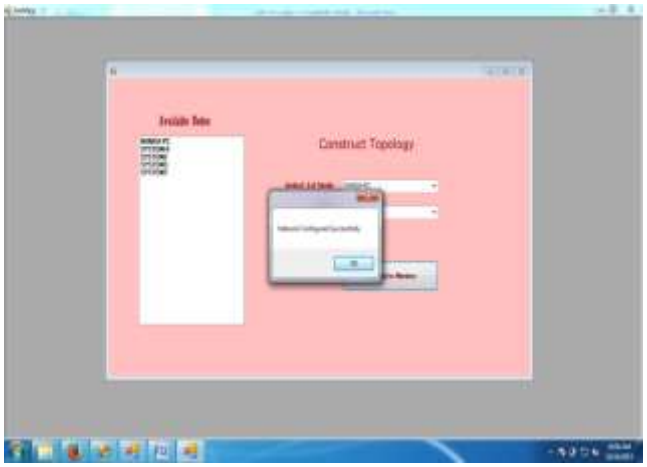

Figure 3: Network Constructing Topology

Figure 4: Sender Encrypt the content and Converting into the packets

Figure 5: Critical Event Monitoring

V. CONCLUSIONS

This paper proposed CEM model for critical event monitoring in wireless ad hoc networks. The correlation between lost packets improves the detection of malicious packet drops. When the number of deliberately lost packets is compared to connection failures, this improvement is visible. Each node must give

reliable packet loss information in order to correctly calculate the correlation between lost packets. Individual nodes may correctly report packet loss using this HLA-based public auditing architecture. This architecture is resistant to collusion, requires considerable processing power at the source, but has low communication and storage overheads. A packet-block-based approach was also proposed to reduce the processing complexity of the baseline creation. Static or quasi-static wireless networks are the only options for ad hoc wireless networks. Because sending packets end-to-end is in their best interests, both the source and destination are truthful in adhering to the protocol.

In the future, link error sinks will be mobile to prolong network lifetime in networks where relocating the sink causes information delay. Because of the problem's combinational complexity, most previous solutions were homomorphic. Create a unified methodology for assessing sink mobility, routing, and latency. Differentiate the induced sub-problems and provide solutions. For the origin problem, provide a polynomial-time optimal technique.

VI. REFERENCES

[1] Tao Shu and Marwan Krunz. “Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, IEEE Transactions on Mobile Computing ,July 2014.Xin Caoy, Gao Congy, Christian S.Jensenz ,Retrieving Top-k Prestige Based Relevant Spatial Web Objects., IJIRCCE/ijircce.2015.

[2] Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

[3] Wenyuam XU, Yanyoung Zhang, Timothy Wood, "The feasibility of launching and detecting jamming attacks in wireless network" in proc. ACM conf. international symposium on Mobile ad hoc networking and computing Urbana-Champaign, IL, USA — May 25 - 27, 2005,pp.46-57. [4] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On Demand Source Routing in Mobile Ad Hoc Networks. Volume: 5, Issue: 1, pp. 1533 - 1546Nov. 2006

[5] Proano and L.Lazos," Packet hiding method for preventing selective jamming attacks” IEEE Transactions on Dependable and Secure Computing, vol. 6, no 1,pp. 101-114, 2012

[6] Monika Nag K J, Mr. S Lokesh, “Detecting Truthfulness of Packet Dropping Attacks Using Public Auditing System in Wireless Ad-Hoc Network”. IJSRD Vol. 3, Issue 04, 2015| ISSN(online): 2321-0613

[7] J. N. Arauz, “802.11 Markov channel modeling,” Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.

[8] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted 0stores,” in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007,pp. 598– 610.

[9] 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. 319–33

[10]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.

[11]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.

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

[13]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.