Mitigating the Protection against Various Types of Attacks in Wireless Ad Hoc Network

Dr. D. Bujji Babu[1] & Ch.Vikas Reddy [2]

[1]Professor, Department of Computer Applications, [2]MCA Scholar

QIS College of Engineering and Technology, Ongole.

ABSTRACT: Ad hoc wireless networks have immense power in a wide diversity of applications. Its inherent weakness, but specific network attacks restrict their broad adaptation in action and delivery. The neighboring nodes in selective drop attack are not cooperative in forwarding the messages to the next node. It is important to recognize the illegitimate node, which will overwhelm the host node and isolate it from the network by keeping its transmission operation. In this paper we deal with one of the hazardous threats, packet loss attack in wireless ad hoc networks. We propose Homomorphic Linear Signature Scheme(HLSS) for effective security against selective drop attack. We analytically researched packet drop rate, jitter and routing overhead using HLSS. Experimental results had shown its successful nature in different network scenarios. We analyzed that packet drop rate was successfully reduced to about 8% rate , jitter to 0.112% rate and routing overhead to 41% rate.

Keywords: Packet dropping, secure routing, attack detection, homomorphic linear signature.

I. INTRODUCTION

Wireless ad hoc networks[1] are a group of computing devices fitted with radio transceivers and interconnected wirelessly via radio frequency without fixed infrastructure or centralized control. Two main wireless ad hoc networking instances are Wireless Sensors Networks and Mobile Ad Hoc Networks.

While wireless ad hoc networks hold promise for a large number of applications in diverse aspects and are expected to revolutionize our everyday lives, the question of protecting such networks has been a major roadblock to their wide-ranging realistic implementation.

Though vulnerable to traditional networks' security threats, these networks are prone to additional intrinsic threats of Ad hoc node features such as narrow communication bandwidth and restricted processing capacity, memory, and power supply [10]. Wireless ad hoc networks are typically implemented in an open and potentially hostile environment, where an attacker can easily seize nodes and use them to attack the network afterwards. The construction of tamper-proof nodes is not guaranteed and subject to the decision of individual users, for example in mobile ad hoc networks, while it is not a feasible or cost-effective solution in large-scale wireless sensor networks.

One of the riskiest attacks on wireless ad hoc networks Is Denial-of - Service (DoS) in which the attacker tries to interrupt the regular use of a resource/service temporarily, indefinitely or permanently.In this paper we deal witha specific type of DoS attack, known as packet drop attack [2], which drops the

packets maliciously by targeting at the message forwarding service in a network environment.It occurs after the attacker successfully places itself in a routing path.

If the attacker removes packets in bulk, it shows up as a Black hole [2] which consumes all the traffic coming in. This sort of packet drop attack is generally referred to as black hole attack. Another type is grey hole attack [2], which occurs when the attacker selectively drops packets. Due to its smarter packet-drop behavior it is harder to detect than black hole attack.

Most research efforts are made during the routing cycle to detect packet drop attackers to prevent the attacks from occurring. In this paper we review identification post-routing. The attacks are carried out on an already defined data communication route via compromised intermediate nodes, either alone or in cooperation.

Connect error and deliberate falling of packets[3] in wireless ad hoc network are two reasons for packet losses. In a highly complex wireless system the detection of selective packet-dropping attacks[3] is extremely challenging. The difficulty comes from the requirement that we not only need to detect the location (or hop) where the packet is dropped, but also to decide if the drop is deliberate or unintentional.

For fact, due to the wireless media's open existence, a packet drop in the network may be triggered by harsh channel conditions (e.g., fading, noise , and interference, a.k.a., connection errors) or by an intruder attacker. Link errors are very common in an open wireless environment, and may not be slightly smaller than an intruder attacker's packet drop rate. So, under harsh channel conditions the intruder attacker will camouflage. In this scenario, it's not enough to correctly determine the exact cause of a packet loss only by analyzing the rate of packet loss.

II.RELATED WORKS

Poongodi T, et al., (2019).[1] had proposed Resistive to Selective Drop Attack (RSDA) scheme which reduced packet drop rate to 9.56% rate and jitter was reduced to 0.115% rate and routing overhead was reduced to 45.49% rate.

Li X, et al., (2011, June).[2] proposed Side Channel Monitoring (SCM) to provide effective defense against selective drop attack in Wireless Ad Hoc Networks. They analytically analyzed the safety intensity of SCM including the detection rate and the number of detected attacks predicted.

Shu T, et al., (2014).[3] Suggested Homomomorphic Linear Authenticator (HLA) based public auditing framework allowing the detector to check the truthfulness of the node-reported packet loss information in Wireless Ad Hoc Networks.

Edemacu K, et al., (2014).[4] They studied some of the packet drop attack detection techniques and evaluated them on a comparative basis; their ability to detect the attack under various attack methods (partial attacks and or cooperate attacks), conditions, and the overheads of computation and communication incurred in the detection process.

Bhalaji N, et al., (2009).[5] had used association based DSR protocol to provide effective security against selective drop attack . They also studied packet drop rate, Throughput, Average Latency, Byte Overheadin MANETS.

Djahel, et al., (2010).[6] studied the effects, challenges, proposals, consequences of Packet Dropping Problem in Mobile Ad Hoc Networks.

Goyal, A. (2014).[7] reviewed different techniques for Selective Packet Drop Attack in MANET.

Balakrishnan, et al., (2005).[8] studied a subset of safe routing protocols, including SAODV, ARAN and Security Aware Ad Hoc Routing, to demonstrate how susceptible they are to packet drop attacks.

X. Meng and T. Chen(2013)[9] suggested a sampled-data event detection technique for linear continuous-time systems, whose output is periodically sampled to be checked for the transmission determination.

H. U. Yildiz et al., (2015)[10] developed and demonstrated a novel Mixed Integer Programming (MIP) architecture and concluded that the optimal node-level strategy will increase the lifespan of the network by more than 20 per cent compared to the optimal strategy at network level.

L. Sánchez-Casado et al., (2015)[11] Suggested ananomaly-based IDS program in MANETs based on an improved windowing approach for collecting and analyzing selected cross-layer functions. The scheme demonstrated a 22% progress in true positive rates and a significant 83% increase in false positive rates compared with previous well-known statistical solutions.

D. Cheelu et al., (2013)[12] recommended a vertical handoff decision plan offering maximum customer satisfaction for the value-based pricing schemes for non-real time mobile multimedia services for market surpluses.

III. PROPOSED SCHEME

There are four phases in HLSS: installation, packet transmission, inspection and surveillance.

3.1 Installation Phase

This process happens right after the creation of a P_{SD} route but prior to the transmission of data packets over the path. In this phase, Source 'S' decides on a symmetric-key crypto-system (e_{key} , d_{key}) and 'K' symmetric keys key_1 , . . . , key_k, where $e_{key}$and $d_{key}$are the keyed encryption and decryption functions, respectively.

Key distribution may be based on the public-key crypto-system such as RSA: 'S' encrypts key_jusing the public key of node $n_j$and sends the cipher text to n_j. $n_j$decrypts the cipher text using its private key to obtain key_j. *'S'* also announces two hash functions, H_1 and H^{MAC}(key), to all nodes in P_{SD}. *H*1 is unkeyed while H^{MAC}(key) is a keyed hash function that will be used for message authentication purposes later on.

Besides symmetric key distribution, S also needs to set up its HLA keys. Let e : G x G -> $G_T$be a computable bilinear map with multiplicative cyclic group G and support Z_p, where p is the prime order of G, i.e., for all α, β ∈ G and q_1, $q_2 \in Z_p$, $e(\alpha^{q1}, \beta^{q2}) = e(\alpha, \beta)^{q1q2}$. Let g be a generator of G. H2(.) is a secure map-to-point hash function: $\{0, 1\}^*$->G, which maps strings uniformly to G. S chooses a random number $x \in Z_p$ and computes $v = g^x$. Let u be another generator of G. The secret HLA key is s_k= x and the public HLA(Homomorphic Linear Authenticator) key is a tuple p_k= (v, g, u).

3.2 Packet Transmission Phase

After completing the setup phase, S enters the packet transmission phase. S transmits packets to P_{SD}according to the following steps. Before sending out a packet P_i, where i is a sequence number that uniquely identifies P_i, S computes $r_i = H_1 (P_i)$ and generates the HLA signatures of $r_i$for node n_j, as follows

$$S_{ji} = [H_2 (i \parallel j)u^{ri}]^x, \text{ for } j = 1, \ldots ,K$$

where || denotes concatenation. These signatures are then sent together with $P_i$to the route by using a one-way chained encryption

that prevents an upstream node from deciphering the signatures intended for downstream nodes. More specifically, after getting $S_{ji}$for j = 1. . .K, Siteratively computes the following:

$S_{Ki} = e_{KeyK}(S_{Ki})$

$T_{Ki} = S_{Ki} \parallel MAC_{KeyK}(S_{Ki})$

$S_{K-1i} = e_{KeyK-1}(S_{K-1i} \parallel T_{Ki})$

$T_{K-1i} = S_{K-1i} \parallel MAC_{KeyK-1}(S_{K-1i})$

3.3. Inspection/Aditing Phase

This phase is triggered when the public auditor $A_d$receives an attack-detection request (ADR) message from *S*. The ADR message includes the id of the nodes on P_{SD}, ordered in the downstream direction, i.e., $n_1, \ldots, n_k$, *S*'s HLA public key information $p_k = (v, g, u)$, the sequence numbers of the most recent *M* packets sent by *S*, and the sequence numbers of the subset of these *M* packets that were received by *D*.

3.4 Surveillance/Detection Phase

The public auditor $A_d$enters the detection phase after receiving and auditing the reply to its challenge from all nodes on P_{SD}. The main tasks of $A_d$in this phase include the following: detecting any over statement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.

IV EXPERIMENTAL SETUP

The experimental configuration uses HLSS on a real machine and tests protocol performance. The HLSS protocol has been implemented on three laptops with the Red Hat Linux operating systems (version 7.4), using Intel i7 processors. We contrasted the achievement of both UCSB and UU RSDA implementations. Simulations of the HLSS results were carried out on static and dynamic scenarios.

The program NETPIPE sends out packets of the size and gives us the following details: time taken to transmit the block, bits / sec throughput, the number of bits in the transferred block and the number of bytes in the transferred block. The information behind the packet size group can be compared and calculated for various packet sizes. Ideally, the throughput of the small packet size is lower and increases to a point after which the packet saturates.

For the static situation, the experiment was performed with different packet size values and the program given the description, network signature and saturation graph. The source code of the program was updated for the dynamic scenario to prevent package size from increasing, and thus for fixed packet sizes the experiment was conducted.

V.RESULTS AND DISCUSSION

The simulation was performed to verify the identification and isolation against gray hole nodes of the proposed scheme. In an area of 1000 m X 1000 m, 60 regular nodes were randomly distributed performing the routing protocol, and one or a few malicious nodes are randomly located which is selectively falling packets. For data communication [9], [10] ten pairs were randomly selected, each sending 5 kb UDP-CBR per second. All standard nodes were pushed with random speeds ranging from 0 to 15 m / s, based on RWM.

5.1. Packet drop rate

The drop rate [11] was increased to around 63.9 per cent when there were randomly fixed gray hole nodes at all pause time at various locations as 5, 10, 15,20 seconds respectively. The cumulative packet drop rate of ABM [12] was 16.7 percent in the presence of gray hole nodes. The drop rate was successfully reduced to about 9.56% rate using RSDA [1]. With the implementation of proposed HLSS, the rate of drop successfully decreased to about 8 percent, as shown in figure 1.

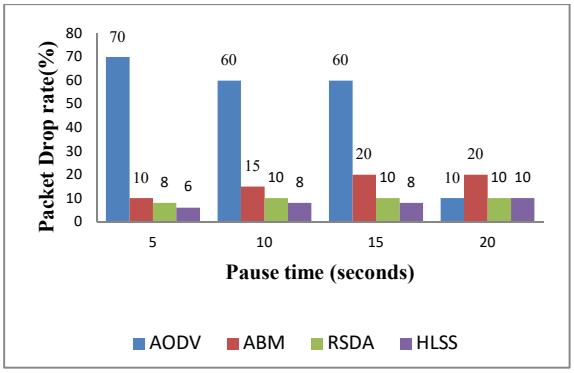

Fig 1: Packet Drop Rate versus Pause Time

5.2. Jitter

Jitter value increased to around 0.56 percent when gray hole nodes were set randomly at various locations at all times of the pause as 5s, 10s, 15s, 20 seconds respectively. The cumulative delay of ABM achieved was 0.14 percent in the presence of gray hole nodes. The jitter rate was effectively reduced to around 0.115 percent with the implementation of RSDA. With the implementation of proposed HLSS the jitter was reduced to around 0.112 percent as shown in figure 2.

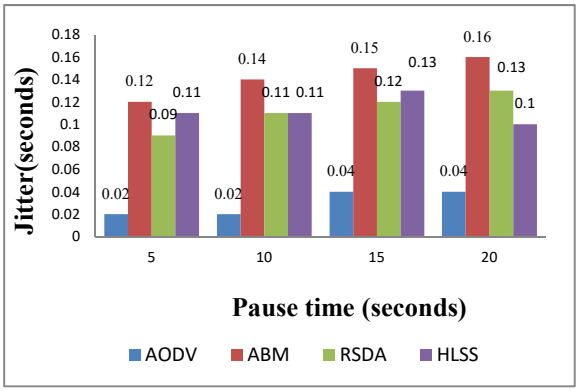

Fig. 2. Jitter vs. pause time.

5.3. Routing Overhead

The routing overhead was increased to around 77.84 percent when gray hole nodes were set randomly at various locations at any point of pause as 5s, 10s, 15s, 20seconds respectively. The routing overhead of ABM was 56.85 percent in the presence of gray hole nodes. The routing overhead was effectively reduced to around 45.49 per cent with RSDA. With the introduction of HLSS the routing overhead was reduced to 41 percent as shown in figure 3.

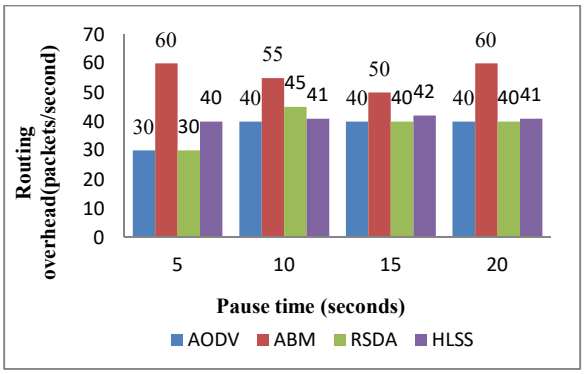

Fig. 3. Routing overhead vs. pause time.

5.4. Packet drop rate for randomly moved gray hole nodes

In addition to 60 distributed normal nodes, 1 or 2 gray hole nodes are considered separately in topology of the network. Next, the gray hole nodes were thought to have been moved randomly. The cumulative packet drop frequency of one gray holes node and two gray hole nodes is shown in the following Figures 4 and 5 and when the nodes are running at varying speeds, the overall packet drop rate is also depicted.

The drop rate for packets is also known as the number of packets which have not reached their destination to the number of packets sent from all network sources. Because of congestion, mobility and traffic without gray hole nodes the network could miss a packet.

In the absence of gray hole nodes, the overall AODV mobility drop rate is approximately 7.93% with random motion of all nodes. If one gray hole node is set in different places, the drop rate rises to around 86.75%. If two gray holes nodes are randomly connected at separate locations, the decrease rate rises to about 94.89 percent in [2][3].

With the deployment of proposed HLSS, the drop rate can successfully reduce by about 11.25% when there is one gray hole node randomly fixed at various positions.

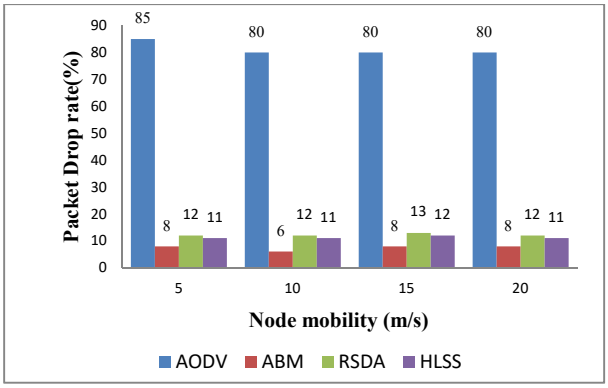

Fig. 4. One gray hole nodes for node mobility *vs.* packet drop rate

With the deployment of proposed HLSS, the drop rate can successfully reduce by about 13.25% when there is two gray hole nodes randomly fixed at various positions.

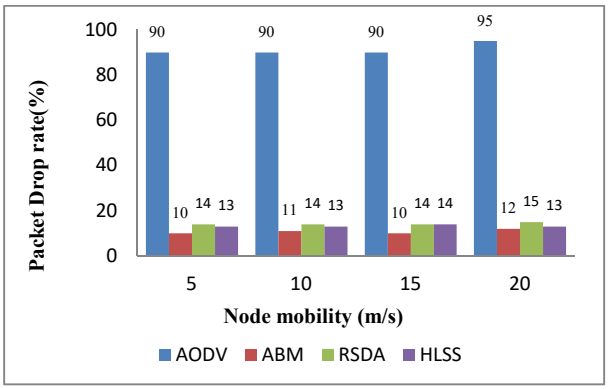

Fig. 5. Two gray holes nodes for node mobility *vs.* packet drop rate

VI. CONCLUSION AND FUTURE SCOPE

HLSS attempts to provide selective drop attack with effective defense. It is necessary to recognize the illegitimate nodes that overload a host and isolate them from the network by keeping its transmission process. Neighboring nodes do not loyally forward their messages to the next node during selective drop attack.

Nonetheless, a malicious node that has entered itself in the path of the data flow may reject unique forwarding messages. There is a need to identify the malicious nodes, which overwhelm a host and fully stop it from running. Therefore, the node that rejects transmission of such messages but sends other messages behaved unpredictably.

The malicious nodes will be refusing to forward messages that move through them in selective drop attack. Finally the attack could theoretically reduce a host's throughput to the minimum level. Security in a WANET setting requires a specific perspective from which security can be established by minimizing the defense from different types of attacks.

REFERENCES

[1] Poongodi, T., Khan, M. S., Patan, R., Gandomi, A. H., & Balusamy, B. (2019). Robust defense scheme against selective drop attack in wireless ad hoc networks. *IEEE access*, *7*, 18409-18419.

[2]Li, X., Lu, R., Liang, X., & Shen, X. (2011, June). Side channel monitoring: Packet drop attack detection in wireless ad hoc networks. In *2011 IEEE International Conference on Communications (ICC)* (pp. 1-5). IEEE.

[3] Shu, T., & Krunz, M. (2014). Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. *IEEE Transactions on mobile computing*, *14*(4), 813-828.

[4] Edemacu, K., Euku, M., & Ssekibuule, R. (2014). Packet drop attack detection techniques in wireless ad hoc networks: a review. *arXiv preprint arXiv:1410.2023*.

[5] Bhalaji, N., & Shanmugam, A. (2009). Reliable Routing against selective packet drop attack in DSR based MANET. *JSW*, *4*(6), 536-543.

[6] Djahel, S., Nait-Abdesselam, F., & Zhang, Z. (2010). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE communications surveys & tutorials*, *13*(4), 658-672.

[7] Goyal, A. (2014). Selective Packet Drop Attack in MANET-A Review. *A Monthly Journal of Computer Science and Information Technology*.

[8] Balakrishnan, V., & Varadharajan, V. (2005). Packet drop attack: A serious threat to operational mobile ad hoc networks. *Networks and Communication Systems*, 18-25.

[9] X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," *Am. Control Conf. (ACC), 2013*, no. 1, pp. 3002–3007, 2013.

[10] H. U. Yildiz, K. Bicakci, B. Tavli, H. Gultekin, and D. Incebacak, "Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies," *Ad Hoc Networks*, vol. 0, pp. 1–23, 2015.

[11] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and R. Magán-Carrión, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping," *Comput. Networks*, vol. 87, pp. 44–58, 2015.

[12] D. Cheelu, M. R. Babu, and P. Venkatakrishna, "A fuzzy-based intelligent vertical handoff decision strategy with maximised user satisfaction for next generation communication networks," *Int. J. Process Manag. Benchmarking*, Dec. 2013.