JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PACKET DROPPING ATTACK IN WIRELESS SENSOR NETWORK USING HLA

C.Durgadevi M.Sc., M.Phil
Assistant Professor
Department of computer science
A.V.P. College of Arts and Science

K.Dejashwini M.Sc., M.Phil
Assistant Professor
Department of computer science
A.V.P. College of Arts and Science

Abstract- Packet Delivery and packet dropping is an important factor of reliability criteria in Mobile ad-hoc Network (MANET). Capability of network can be examined through these factors also considered for transmission of information but analyze and achieve the maximum accuracy of packet loss and their source of packet loss is a critical decisive factor. In wireless networks, the three aspects such as traffic, link errors and malicious nodes are affecting the packet delivery of transmission in both static and dynamic networks but achieving packet drop rate is not in accurate manner. To solve this issue, number of algorithms could be implemented in existing system to achieve accurate packet loss rate over the delivery report and packet loss gathered from nodes in static or quasi static networks with confidentiality of information as well as certainty of detection. So with that motivation, we proposed to calculate accurate packet loss detection based on malicious node and link errors in dynamic networks. This network is highly infrastructure less network so malicious node and link errors are extremely available compared with static networks. We construct the EHLA (Enhanced Homomorphic Linear Authenticator) to supervise and identify the packet loss rate at precisely in MANET exclusive of less privacy issues. During this accomplishment we attain low communication, storage overhead and energy Consumption

I.INTRODUCTION

A Wireless ad hoc network is a collection of heterogeneous network node forming the temporary networks without the aid of any infrastructure or any centralized administrator. In such an environment, it may be necessary for one wireless host to enlist the aid of other hosts in forwarding a packet to its destination; this is because of the limited range of each wireless host‘s transmission. Wireless ad hoc networks (WANETs) Figure 1 do not rely on any fixed infrastructure but communicate in a self-organized way. Accordingly, a good ad hoc routing protocol should also be scalability and reliable is major concern. There are quite a number of uses for wireless ad hoc networks. For example, the military can track an enemy tank as it moves through the geographic area covered by the network. Your local community can use an ad hoc network to detect your car moving though an intersection, checking the speed and direction of the

car. In an environmental network, you can find out the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations.

These devices are now playing an ever-increasingly important role in our lives. To mention only a few examples, now a days wireless users can rely on their cellular phone to check e-mail and browse the Internet; travelers with portable computers can surf the internet at airports, railway stations, cafes, and other public locations; tourists can use Global Positioning System terminals installed inside rental cars to view driving maps and to locate tourist attractions, files or other information can be exchanged by connecting portable computers via Wi-Fi and other wireless technology like Bluetooth and chirping technology in the latest phone of the apple after apple-3 series of company phone. While attending conferences or meetings and celebrating occasions, and at home, a family can synchronize data and transfer files between portable devices and desktops.

The cost of the technology downing in the fold, now we can see that the mobile devices getting smaller, cheaper, more convenient, and more powerful, they also run more applications and network services. All of these factors are fueling the explosive growth of the mobile computing equipment market seen today.

While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the very nature of radio transmissions, which are made on the air.

On a wired network, an intruder would need to break into a machine of the network or to physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer (and possibly a directional antenna).

There is a wide range of tools available to detect, monitor and penetrate an IEEE 802.11 network, such as NetStumbler, AiroPeek, Kismet, AirSnort, and Ethereal. Hence, by simply being within radio range, the intruder has access to the network and can easily intercept transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street eavesdropping on the communications inside a nearby building.

As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise.

Packet Dropping Attack

Mobile Ad Hoc Network (MANETs) is a network of mobile nodes which can move freely. These nodes have characteristic that they can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. MANETs are highly dynamic network because nodes may join and leave the network at any time.

The Ad hoc on demand distance vector routing is a reactive routing protocol that finds the route on demand i.e. when one node wants to send message to another node. The different network layer attacks such as worm hole attack, black hole attack, packet dropping and message tampering attack causes network operation disturbance. Security at network layer can be provided using different approaches. These approaches used to detect and prevent such attacks in MANET. In this thesis we review some techniques that have prevented such attacks.

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of

that network, then it effectively separates the network in to two disconnected components.

In this attack two things are take place. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.

However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrong doing.

This attack causes direct interruption to the routing message. In this attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behavior remain concealed.

Security in MANETS is such a hot topic among the research communities, if it is assured properly it can be used as a success factor and for the widespread deployment of the network. Several types of attacks in network layers have been identified and analyzed recently in most of the research work. Security countermeasures and the defense against for each of the network attacks so far designed and implemented for MANETS are presented in the above sections. The research proposals till date, in MANETS are based upon a specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research can be done on the robust key management system, trust-based protocols, integrated approaches to routing security, and data security at network layer

In this thesis we have introduced the MANET network and classification of routing used in MANET. The different MANET attacks on network layer disturb the networking operation.

AODV routing protocol finds route from source to destination. But if the malicious node is present in network it does not allow routing messages to properly send to other nodes in network. So the security mechanism that prevents such attacks is required.

The security mechanism can be evaluated by different security criteria. In this thesis we reviewed some of techniques that prevent the network layer attacks. Some techniques used to detect network layer attacks in parallel and some of are designed for preventing some specific attacks.

In MANET, a packet dropping attack is a type of denial of service in which a node in the network will drop the packets instead of forwarding them, the packet dropping attack is very hard to detect and prevent because it occurs when the node becomes compromised due to a number of different causes.

The packet dropping attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

II. RELATED WORKS

Wireless ad-hoc networks are widely used because these are very easy to deploy. However, there are various security issues and problems. Two most important issues are interoperability and interaction among various security technologies which are very important to consider for configuration and management point of view. The packet drop ratio in the wireless network is

very high as well as packets may be easily delayed by the attacker. It is very difficult to detect intruders, so it results into high false positive rate. Packets may be dropped or delayed by intruders as well as external nodes in wireless networks. Hence, there is the need of effective intrusion detection system which can detect maximum number of intruders and the corresponding packets be forwarded through some alternate paths in the network. In this paper we propose an alternate solution to detect the intruders/adversary with help of trust value. It would remove the need of inbuilt IDS in the wireless networks and result into improving the performance of WLAN.

The security exertion and security threats in the wireless networks are increasing, particularly in varied-frightening hazard, such as hacker attacks, worms, Trojans, DOS attacks etc. being serious troubles to the user. To tackle this problem, a new scheme: WBIPS (WTLS-Based IPS) replica is proposed. In this model, a coherent solitary path is build connecting each wireless terminal and its destination. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for discovery of a path to the target in wireless ad-hoc networks [19]. When the source node requests to create an association with the destination node, it televises an RREQ message.

In ad-hoc networks that employ the AODV protocol, the intruder node suck up the network passage and fall all the corresponding packets. To explain the Packet Drop Attack, we include a malicious node that demonstrates Black Hole activities in the set-up. We illustrate the packet drop attack with help of given scenario shown in Figure 1. We suppose that Node 3 is the malicious node. When Node 1 televise the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that contain the maximum sequence number of Node 4, as if it is coming from Node 4. Node 1 presumes that Node 4 is following Node 3 with 1 hop and discards the recently arrived RREP packet coming from Node 2. Subsequently, Node 1 begin to discharge its data packet to the node 3 expecting that these packets will arrive at Node 4 but Node 3 will slump all data packets.

In a Packet Drop Attack, after a while, the starting nodes realize that there is a linkage fault since the acceptance node refusing to transmit TCP ACK packets. If it dispatch away fresh TCP data packets and find out a fresh route for the target, the malicious node still handle to cheat the sending node.

If the sending node releases UDP data packets, the difficulty is not identified since the UDP data connections do not hang around for the ACK packets.

Wireless networks are very easy to deploy because there is no need to establish any physical path. This feature of wireless network results into birth of various attacks.

In the Packet drop attack, the attacker targets some nodes in the wireless network and then drop the packets sent towards the intended nodes. Attackers try to drop/delay the packets in the routine manner so it's very difficult to detect.

The packet drop will further results into the high false positive rates and ultimately breaks the security of wireless networks. So, our problem is to detect the Packet drop attack and try to reduce the packet drop ratio so that it will result into law false positive rates.

PACKET SINKING: A malicious node slump all or a few of the packets that is believed to be forward. It can also sink the data produced by itself on behalf of some malicious intention for instance.

PACKET AMENDMENT: A malicious node alters the entire or a few of the data packets that is made-up to forward.

It can also modify the data it produce to defend it from being recognized or to lay blame on former nodes. In previous Black hole detection techniques, black hole node is randomly chosen based on the number of packet dropped.

So, sometime legitimate user also treated as the intruders or attacker. It will result into high false positive rate and it violates the security of wireless networks.

TRUST VALUE ALGORITHM: The proposed algorithm is based on the trust values of individual nodes. Initially, all the nodes of wireless ad-hoc network have zero trust value.

The malicious nodes in a route can intentionally drop the packets during the transmission from source to destination. It is difficult to distinct the packet loss due to link errors and malicious dropping. Here is a mechanism which will detect the malicious packet dropping by using the correlation between packets. An auditing architecture based on homomorphism linear authenticator can be used to ensure the proof of reception of packets at each node.

III. PROBLEM DEFINITION

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.

IV. PROPOSED SYSTEM

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., reflects 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. Routing in an ad-hoc 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.

Nodes are co operatively function in the routing path. An attacker uses this cooperation and pretends to be an one of the node in the routing path. Once the attacker included in the routing path starts discarding the packet. The intrusion node stops sending the packet received from the above node to the node below which completely disturb the routing path between the sender and receiver. This type of attack is known as DoS. The malicious node may classify the significance of different packets and discard the most significance packet which leads to degradance of the network performance the authors in Identifying the significant packet is a critical task in a wireless medium. In this thesis we develop an absolute algorithm for identifying the most significant packet discard made by the inside intruder. Our algorithm provides truthful and publicly verifiable decision by the auditor. The accurate detection is obtained by the correlations between the lost packets. The correlations are performed by Auto correlation function [ACF]. To verify the lost packets and the information send by the individual node about the packet loss is checked by constructing Homomorphic linear Authenticator. HLA is a signature scheme and is based on 4 ppt algorithm that provides privacy, collusion avoidance and low storage overheads.As described in the next section, previous work on distinguishing between causes for dropped packets considered only collisions and channel errors and ignored malicious packet drops. On the other hand, protocols that detect malicious packet dropping ignored collisions and channel errors.

In this thesis we adopt a unified approach to packet loss considering collisions, channel errors, and malicious packet drops. We consider two possibilities for a malicious node. First, it aims to disrupt network operation by not relaying a packet to the next hop. In this case the node will acknowledge the packet to the sender.

The aim of attacker is to degrade the network performance by dropping or discarding the packet. Malicious packet discarding can be any type (ie) it may be a significant packet or random packet. There may be some collision between malicious node. So, a malicious node may establish separate routing path apart from the original routing path and transmits its packet to the below malicious node this form of exchange can't be dected by the auditor.

HLA Process. Consider a multi-hop network which is having an arbitrary path PSD as. The source node sends the packets through intermediate nodes to the destination node. In each hop, the sending node is called as an upstream node of an receiving node.

The packets are transmitted from source to destination and a bitmap is obtained for each node as (a 1,a2….am) where aj=0 or 1. If the packet is successfully transmitted then aj=1 and if the packet is not transmitted the value of aj is considered as 0. By using this bitmap we can find the correlation between the lost packets. From this correlation we can find the malicious node

Homomorphic linear au thenticator (HLA) a cryptographic method which is used in cloud computing. In this type of scheme, source is allowed to generate the HLA signatures s 1,…,sM for M messages r1,…,rM.

The source sends these signatures si's and packets ri's along the route. The node will create a valid HLA signature if and only if it has received all the signatures. Since si's and ri's are sent together, the reception of signatures ensure that all the packets are transmitted without getting dropped. In this way we can truthfully detect the malicious node.

V. PROPOSED MECHANISM WORK PHASES

This mechanism includes 4 phases

i)Setup phase: After the establishment of route, this phase takes place. It is before any packet is transmitted to the route. Source makes use some symmetric key cryptosystem to generate encryption, decryption and K number of symmetric keys for K intermediate nodes. Source uses encryption and decryption method to provide symmetric keys to the nodes.

This phase takes place right after route PSD is established, but before any data packets are transmitted over the route. In this phase, S decides on a symmetric-key crypto-system (encryptkey, decryptkey) and K symmetric keys key1, . . . , keyK, where encryptkey and decryptkey are the keyed encryption and decryption functions, respectively. S securely distributes decryptkey and a symmetric key keyj to node nj on PSD, for j = 1, . . . , K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts keyj using the public key of node nj and sends the cipher text to nj . nj decrypts the cipher text using its private key to obtain keyj . S also announces two hash functions, H1 and HMAC key , to all nodes in PSD. H1 is unkeyed while HMAC 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 × G → GT be a computable bilinear map with multiplicative cyclic group G and support Zp, where p is the prime order of G, i.e., for all α, β ∈ G and q1, q2 ∈ Zp, e(α q1 , βq2) = e(α, β) 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 ∈ Zp and computes v = g x . Let u be another generator of G. The secret HLA key is sk = x and the public HLA key is a tuple pk = (v, g, u).

ii)Packet transmission phase: After the completion of setup phase, source generates signatures and add these signatures to the packets and send to the route. Each node stores signature for the proof of reception in its database for the future purpose.

Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes ri = H1(Pi) and generates the HLA signatures of ri for node nj , as follows

$$sji = [H2(i||j)u\ ri\ ]\ x\ , \text{ for } j = 1, \ldots, K$$

where || denotes concatenation. These signatures are then sent together with Pi 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 sji for j = 1, . . . , K, S iteratively

Computes the following: s˜Ki = encryptkeyK (sKi)

τKi = ˜sKi||MACkeyK (˜sKi)

s˜K−1i = encryptkeyK−1 (sK−1i||τKi)

τK−1i = ˜sK−1i||MACkeyK−1 (˜sK−1i) . . .

s˜ji = encrypt keyj (sji||τj+1i)

τji = ˜sji||MACkeyj (˜sji) . . .

s˜1i = encryptkey1 (s1i||τ2i)

τ1i = ˜s1i||MACkey1 (˜s1i)

where the message authentication code (MAC) in each stage j is computed according to the hash function HMAC keyj . After getting τ1i, S puts Pi||τ1i into one packet and sends it to node n1.

When node n1 receives the packet from S, it extracts Pi, s˜1i, and MACkey1 (˜s1i) from the received packet. Then, n1 verifies the integrity of ˜s1i by testing the following equality:

MACkey1 (˜s1i) = H MAC key1 (˜s1i).

If the test is true, then n1 decrypts ˜s1i as follows:

decryptkey1 (˜s1i) = s1i||τ2i.

Then, n1 extracts s1i and τ2i from the decrypted text. It stores ri = H1(Pi) and s1i in its proof-of-reception database for future use. This database is maintained at every node on PSD. It can be considered as a FIFO queue of size M, which records the reception status for the most recent M packets sent by S. Finally, n1 assembles Pi||τ2i into one packet and relays this packet to node n2. In case the test in fails, n1 marks the loss of Pi in its proof-of-reception database and does not relay

the packet to n2. The above process is repeated at every intermediate node nj , j = 1, . . . , K. As a result, node nj obtains ri and its HLA signature sji for every packet Pi that the node has received, and it relays Pi||τj+1i to the next hop on the route. The last hop, i.e., node nK, only forwards Pi to the destination D. As proved in Theorem 4 in Section 4.3, the special structure of the one-way chained encryption construction in (4) dictates that an upstream node on the route cannot get a copy of the HLA signature intended for a downstream node, and thus the construction is resilient to the collusion model defined in Section 3.2. Note that here we consider the verification of the integrity of Pi as an orthogonal problem to that of verifying the tag τji. If the verification of Pi fails, node n1 should also stop forwarding the packet and should mark it accordingly in its proof-of-reception database.

iii) Audit phase: This phase comes into picture when auditor receives ADR message from the source. Each node sends the bitmap of packet received and also the signature and it compares the signatures with the stored signatures. If it is correct then it will prove that node has received all the packets. Here node cannot tell that it has received a packet when it does not receive it.

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1, . . . , nK, S's HLA public key information pk = (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. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest. Ad conducts the auditing process as follows.

Ad submits a random challenge vector cj = (cj1, . . . , cjM) to node nj , j = 1, . . . , K, where the elements cji's are randomly chosen from Zp. Without loss of generality, let the sequence number of the packets recorded in the current proof-of-reception database be P1, . . . , PM, with PM being the most recent packet sent by S. Based on the information in this database, node nj generates a packet-reception bitmap bj = (bj1, . . . , bjM), where bji = 1 if Pi has been received by nj , and bji = 0 otherwise. Node nj then calculates the linear combination r (j) = ∑M i=1,bji≠0 cjiri and the HLA signature for the combination as follows:

$$s(j) = \prod_{i=1,b_{ji}\neq 0} s_{ji}^{c_{ji}} .$$

Node nj submits bj , r (j) , and s (j) to Ad, as proof of the packets it has received. Ad checks the validity of r (j) and s (j) by testing the following equality: e(s (j) , g) = e(∏M i=1,bji≠0 H2(i||j) cjiu r (j) , v).

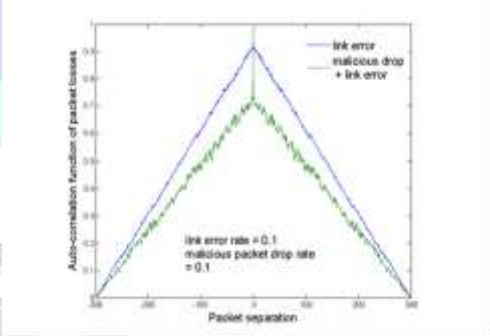
iv)Detection phase: The auditor goes for this phase after receiving reply from the nodes. First it checks for the overstatement of packet loss using the bitmap sent by the nodes. In the beginning per hop packet loss bitmap is calculated from one node to other node by applying the complement of XOR operation for the bitmap of two successive nodes. At last it calculates the autocorrelation to find whether there is malicious node in the network or not.

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement 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. More specifically, Ad performs these tasks as follows. Given the packet-reception bitmap at each node, b1, . . . , bK, Ad first checks the consistency of the bitmaps for any possible overstatement of packet losses. Clearly, if there is no overstatement of packet loss, then the set of packets received at node j + 1 should be a subset of the

packets received at node j, for j = 1, . . . , K − 1. Because a normal node always truthfully reports its packet reception, the packet-reception bitmap of a malicious node that overstates its packet loss must contradict with the bitmap of a normal downstream node. Note that there is always at least one normal downstream node, i.e., the destination D. So Ad only needs to sequentially scan bj 's and the report from D to identify nodes that are overstating their packet losses. After checking for the consistency of bj's, Ad starts constructing the per-hop packet-loss bitmap mj from bj−1 and bj . This is done sequentially, starting from the first hop from S. In each step, only packets that are lost in the current hop will be accounted for in mj . The packets that were not received by the upstream node will be marked as "not lost" for the underlying hop. Denoting the "lost" packet by 0 and "not lost" by 1, mj can be easily constructed by conducting a bit-wise complement-XOR operation of bj−1 and bj . For example, consider the following simple case with three intermediate nodes (four hops) on the route and with M = 10. Suppose that b1 = (0, 1, 1, 1, 1, 1, 1, 1, 0, 1), b2 = (0, 1, 1, 1, 1, 1, 1, 1, 0, 1), b3 = (0, 1, 0, 1, 1, 0, 1, 1, 0, 1), and the destination D reports that bD = (0, 1, 0, 1, 1, 0, 1, 1, 0, 1). Then the per-hop packet-loss bitmaps are given by m1 = (0, 1, 1, 1, 1, 1, 1, 1, 0, 1), m2 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1), m3 = (1, 1, 0, 1, 1, 0, 1, 1, 1, 1), and m4 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1). The auditor calculates the autocorrelation function γj for each sequence mj = (mj1, . . . , mjM), j = 1, . . . , K, as follows

The relative difference ϵj is then used as the decision statistic to decide whether or not the packet loss over the jth hop is caused by malicious drops. In particular, if ϵj ≥ ϵth, where ϵth is an error threshold, then Ad decides that there is malicious packet drop over the hop. In this case, both ends of the hop will be considered as suspects, i.e., either the transmitter did not send out the packet or the receiver chose to ignore the received packet. S may choose to exclude both nodes from future packet transmissions, or alternatively, apply a more extensive investigation to refine its detection. For example, this can be done by combining the neighbor-overhearing techniques used in the reputation system. By fusing the testimony from the neighbors of these two nodes, Ad can pin-point the specific node that dropped the packet. Once being detected, the malicious node will be marked and excluded from the route to mitigate its damage. The above detection process applies to one end-to-end path. The detection for multiple paths can be performed as multiple independent detections, one for each path. Although the optimal error threshold that minimizes the detection error is still an open problem, our simulations show that through trial-and-error, one can easily find a good that provides a better detection accuracy than the optimal detection scheme that utilizes only the pdf of the number of lost packets.

VI. EXPERIMENTAL RESULTS



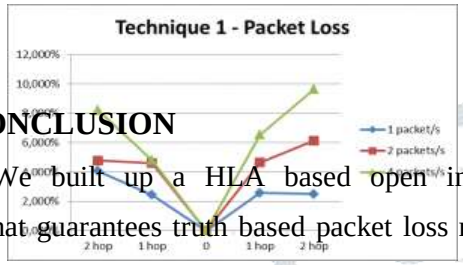
Comparison of correlation of loss

To correctly calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. Where the threshold zth is the solution to the equation h0 ð zth Þ ¼ h1ðzthÞ. The problem with this mechanism is that, when the mean of y is small, h1 ðz Þ and h0 ðz Þ are not sufficiently separated, leading to large Pfa and Pmd, This observation implies that when malicious packet drops are highly selective, counting the number of lost packets is not sufficient to accurately differentiate between malicious drops and link errors. For such a case, we use

the correlation between lost packets to form a more informative decision statistic.

Packet Loss

In communication, the nodes can communicate with each other, even if there's a low performance. Also to be taken in consideration is the offered load in the network. In most of Ad-Hoc it is not required that the sensors transmit their information at rates higher than one packet per second. Most of the time the sensors are in sleep mode, only sending their sensing data once in a while.



VII. CONCLUSION

We built up a HLA based open inspecting design that guarantees truth based packet loss reporting by individual nodes. This engineering is conspiracy verification, requires moderately high computational limit at the source nodes, however causes low correspondence and capacity overheads over the course. To lessen the calculation overhead of the standard development, a bundle square based component was additionally proposed, which permits one to exchange location exactness for lower calculation many-sided quality. Some open issues stay to be investigated in our future work. In the first the proposed system constrained to static or quasi-static wireless ad hoc. Visit changes on topology and connection attributes have not been considered. In this thesis we have expected that source and goal are honest in taking after the set up convention in light of the fact that conveying bundles end-to-end is to their greatest advantage. Acting up source and goal will be sought after in our future research. Additionally, in this thesis, as a proof of idea, we for the most part centered on demonstrating the achievability of the proposed cypto-primitives and how second order insights of packet loss can be used to enhance recognition exactness. As an initial phase in this bearing, our investigation mostly accentuate the basic components of the issue, for example, the untruthfulness way of the aggressors, people in general certainty of evidences, The randomness of wireless channels and packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in our future studies.

REFERENCES

[1] Intrusion Detection Algorithm for Packet Loss Minimization in Wireless Sensor Networks s.Rizwana,Thangadurai Natarajan Research gate, 2019

[2] Simulation of Wireless Sensor Network Security Model Using NS2; Nayana Hegde, Dr.Sunilkumar S.Manvi, International Journal of Latest Trends in Engineering and Technology, 2014

[3] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008 .

[4] Philipp Hurni and Torsten Braun "Energy-Efficient Multi-Path Routing in Wireless Sensor Networks" 7th International Conference, September 10-12, 2008.

[5] Tao Shu and Marwan Krunz "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks" IEEE Transactions on Mobile Computing DOI:10.1109/TMC.2014

[6] W. Kozma Jr. and L. Lazos. REAct: resource-efficient answerability for node misconduct in circumstantial networks supported random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009 .

[7] W. Kozma Jr. and L. Lazos. coping with liars: misconduct identi-fication via Renyi-Ulam games. In Proceedings of the International ICST Conference on Security and Privacy in Communication Networks (SecureComm), 2009

[8] A. Proano and L. Lazos. spot jamming attacks in wireless networks.In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.

[9] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor: ascendable secure routing for circumstantial networks. In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, march 2010

[10] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in Proc. 2003 Conf. IEEE Computer Commun., pp. 1713–1723