Diagnosis of Packet dropping attacks in Wireless Ad Hoc Networks with Secure Routing and High Detection Accuracy

Shraddha Chougule[1], Shivanjali Desai[2], Prof. Ketaki Bhoyar [3]
Department of Computer Engineering
[1,2]Dr. D.Y .Patil Institute of Engineering Management & Research Akurdi, Pune, Maharashtra
[3]Assistant Professor,Dr. D.Y .Patil Institute of Engineering Management & Research Akurdi, Pune, Maharashtra

Abstract-*We have implemented a framework for detecting selective packet drops made by insider invaders. Goals achieved in this construction are privacy perseverance, also it incurs low communication and storage overheads. Large scale sensor networks are deployed by numerous application and for decision making purpose bundles perceived by the networks are used in substructure. The bundles travel from source to destination along in-between nodes. There are chances of introducing malicious invaders as dummy nodes can track the information and also features packet drop attacks by these malicious data forwarding nodes in the network. Hence assuring the high data reliability prominent decision making is needed. The challenging factors of high data reliability management for sensor networks are efficient storage, low energy and bandwidth consumption and secure transmission. This efficient mechanism will ensure diagnosis of forgery nodes by investigation and preserves the high data reliability.*

Verifying the reliability is necessary because sometimes invader reports false information to evade being diagnosed hence to ensure the packet loss information reported by individual node is truthful or not Homomorphic Linear Authenticator (HLA) based detector is used. To provide secure routing Advanced Encryption Standard (AES) algorithm is used providing end to end encryption.

Keywords-Packet dropping, AES (Advanced Encryption Standard), Attack detection, Link Error, Homomorphic Linear Authentication etc.

I. INTRODUCTION

A mobile ad hoc network (MANET), also known as wireless ad hoc network or ad hoc wireless network. Each device in a MANET is free to move separately in any direction hence its links to other devices frequently. There are some limitations of the Wireless Ad hoc network i.e. Packet loss due to transmission errors, variable capacity links , frequent disconnections , limited communication bandwidth , dynamically changing topologies [2].

It can be formed either by mobile nodes or by both fixed and mobile. Nodes are randomly connected with each other and forming different topology. They have ability to self-configure makes this technology suitable for crisis areas where there is no communication infrastructure for emergency search and rescue operations where a network connection is urgently required. There are different types of attacks present in MANET which makes disturbances in networks while transferring packet from source to destination. These attacks are as below:

Passive Attacks:

Passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is simply to gain information about the target and no data is changed on the target. The passive attacks are difficult to detection. In its, operations are not affected. Type of passive attacks:War driving, dumpster diving,

Active Attacks:

Active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. It involves modification, disruption and affects the operation of the network. Type of active attacks is masquerade attack, session replay attack.

External Attack:

The external attack is conceded out by the nodes which do not belong to network. It may cause unavailability and congestion by sending false information for the network jamming attack.

Internal Attack:

Internal attacks is conceded out by the node which is part of interconnect network. In an internal attack from the network the malicious node gains unauthorized access and

behave as a genuine node. Traffic can be analyse between other nodes and may participate in the activities of other networks like black hole, selective packet drop attack etc.

In this paper, we have developed an accurate algorithm for detecting malicious packet drops and the place at which packet drop takes place and again data transferring start from node which is previous to that place. Our aim is to preserve privacy and provide truthful detection. By utilizing the reciprocity between the positions of lost packets, as calculated from the Autocorrelation Function (ACF) the detection accuracy is improved. By detecting the reciprocity between lost packets, one can decide whether the packet loss is purely due to regular link errors or due to malicious node present in network. To guarantee the packet loss information reported by individual node is truthful or not by node Homomorphic Linear Authenticator (HLA) based detector is used. Verifying the truthfulness is necessary because sometimes invader reports false information to evade being diagnosed. For example, some packets may have been dropped by the node but the node reports that these packets have been forwarded. Therefore, this mechanism ensures the verification and the truthfulness of the reported information.[1]

II. LITERATURE SURVEY

Tao Shu et. al, proposed a mechanism that generate randomized multipath routes. They have explained a multipath scheme where once an invader obtains the routing algorithm, it can it can compute the same routes known to the source, and hence imperil all information sent over these routes. Routes traversed by each packets are cannot be recognize by the invader. The routes generated by this mechanism are quite capable of passing over black holes at low energy cost making them highly dispersive and energy-efficient. It is an highly expensive method as extensive simulations are to be conducted. [3]

Loukas Lazos et. al, proposed Jamming Attacks in the paer entitled “Packet-Hiding Methods for Preventing Selective Jamming Attacks”. In this paper, under an internal threat model the problem of jamming is explained. The invader targets on “high importance” messages by misusing the internal knowledge for launching selective jamming attacks. The computational and communication overhead is an issue because the packet hiding Methods are based on several cryptographic primitives. [8]

S. Buchegger et. al, proposed some new strategies on trust administration in MANETs. They have given overview of trust based conventions. MANET is a network has many free or autonomous hubs. As they are free to move, they has no altered topology. To route bundles every one of the hubs must co-work with each other. They should consider social, data and correspondence systems, and consider the serious asset imperatives (e.g., registering power, vitality, transfer speed, time), and progression (e.g., topology changes, portability, hub disappointment, spread channel conditions). [9]

Kennedy Edemacu et. al, proposed Packet drop attack detection techniques. Techniques based on reputation module, route discovery module, audit modules referred as the AMD system are explained. Functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers are coordinated by closely interaction of these modules. [5]

III. PROPOSED SYSTEM

A. System Architechture

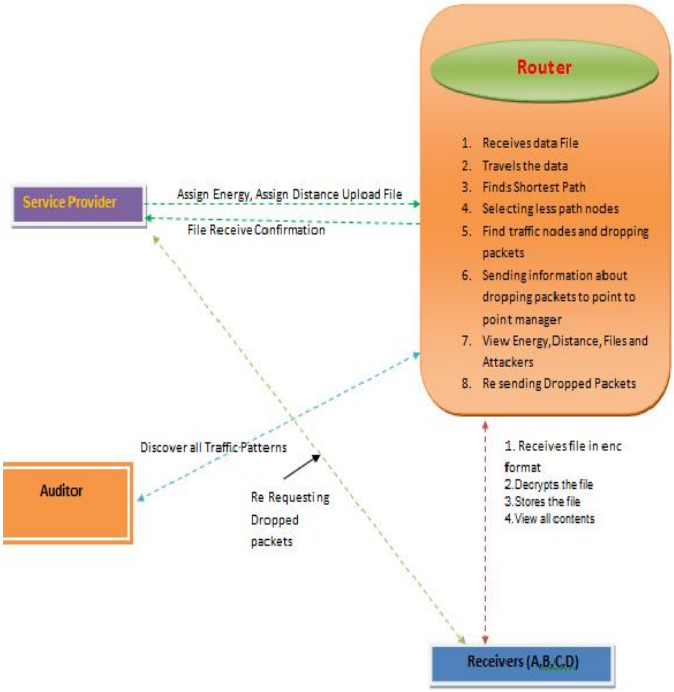

Fig-1: System Architecture

- Service Provider:

In this module, the service provider browses the file and sends to the particular end users via router. And also service provider can assign energy and assign distances for the nodes in router.

- Router:

In this module, by selecting shortest distances between two nodes & sufficient node energy file is sent from source to destination (from service provider to end users) by the router. And if node has less energy than file size then packet dropper in router drops the some packets from file and sends remaining file to the destination. And the operations like view files, view attackers, verify, refresh, view distances, view energy are also done by it.

- Auditor:

In this module, the auditor discovers the traffic pattern, means it stores the details of dropped packets. It contains details of in which node packets are dropped, how many no of packets dropped, from which file dropped & status of packets.

Destination (End User):

In this module, there are n no of destinations (A, B, C….).These end users only receive the file from service provider via router. While getting the file from service provider there may be chances of packets dropping, if packets are dropped then end user will gets dropped packets from point to point manager. The end users receive the file by without changing the File Contents. Users may receive particular data files within the network only.

Attacker:

Attacker is one who makes changes the energy of particular nodes in router. And all attackers' details stored in router with their all details such as attacker Ip address, attacked node, modified energy and attacked time.

B. Homomorphic Linear Authenticator(HLA)

It improves the detection accuracy by calculating the correlation between lost packets with the help of auto correlation function of the bitmaps at each node in the route. Bitmap describes the lost status of each packet in the transmission. The basic idea is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the correlation pattern is different.

To get the correct correlation, the truthfulness of the packet loss bitmaps is essential. In order to ensure the correctness the system uses a public auditing approach. The auditor uses a variation of the cryptographic primitive called homomorphic linear authenticator (HLA).

IV. ALGORITHMIC APPROACH

A. AES(Advanced Encryption Standard)

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted.

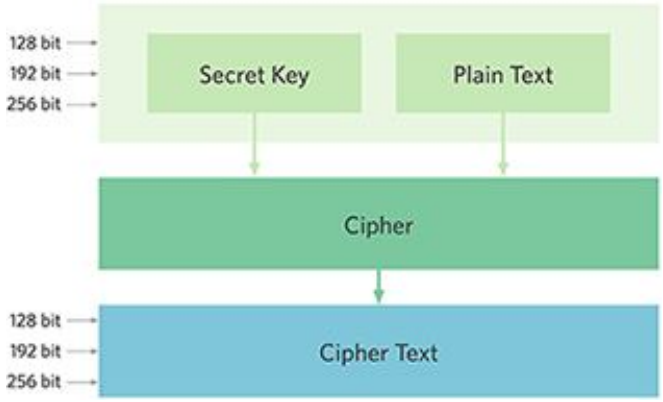

Fig-2: AES Working

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.

V. RESULTS AND DISCUSSION

The given research is implemented in Java in two different cases. Firstly, it can be simulated as in Normal Case and Second, as Attacker Case. In normal case, simulation will be done from source to destination for forwarding packet without dropping in between the route. Whereas in case of attacker case, there are two different possibilities to drop the packets in between. They are, 1) If Node have less Bandwidth 2) If Node is failure in between the selected route.

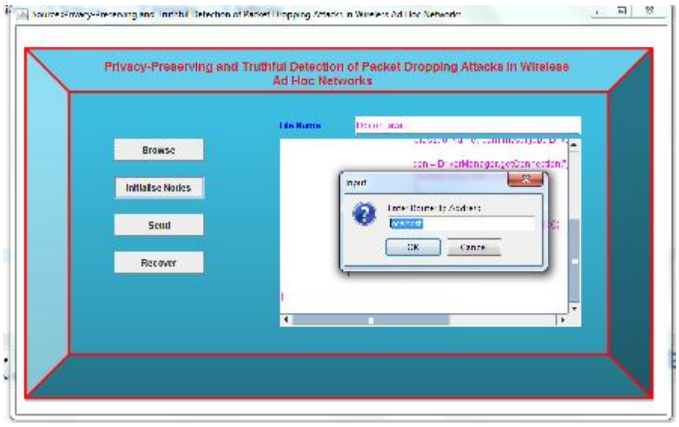

Fig-3: Source Page

The above figure, shows source page where the file can be uploaded for disseminating the packets from source to destination by selecting network IP address.

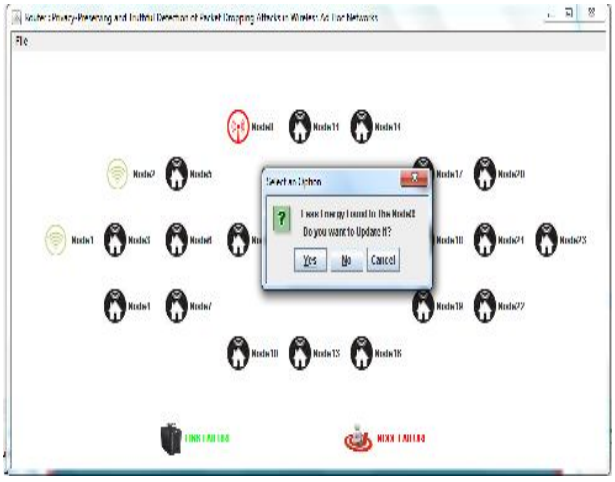

Fig-4: Node Failure

Figure.2, represents, the packet dropped because of node failure. Whenever there ia node failure, it will ask for updating the node. Once node updated, simulation will start from previous node i.e where failure occurred to destination instead of source node .

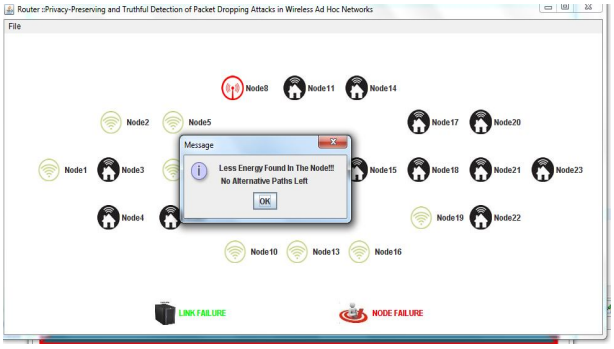

Fig-5: Bandwidth Assigned to Node

Above figure, indicates, if there is a low bandwidth on the node the packet will be dropped and will show there is no alternative path to transmit packet.

V. CONCLUSION

In this paper, we showed that compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves 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, it is critical to acquire truthful packet-loss information at individual nodes. We developed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy-preserving requirement for the auditing process, and 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.

ACKNOWLEDGEMENT

We would like to take this opportunity to thank our internal guide Prof. Ketaki Bhoyar for giving us all the help and guidance we needed. We are really grateful to her for her kind support. Her valuable suggestions were very helpful. We are also grateful to Prof. P. P. Shevatekar & Mr. Nareshkumar R.M, DYPIEMR, Akurdi for their indispensable support and suggestions.

REFERENCES

[1] Shraddha Chougule, Shivanjali Desai, Ketaki Bhoyar - Packet Dropping Attacks in Wireless Ad Hoc Networks Using Privacy Preserving And Truthful Detection(IJRISE), Vol. 5 ,30 January 2017.

[2] Nareshkumar R.M, "Computational Intelligence Based Efficient Routing in MANET: A Review", International Journal for Research in Engineering Application & Management (IJREAM), ISSN : 2494-9150 Vol-02, Issue 04, July 2016., pp.28-34.

[3] Tao Shu and Marwan Krunz Privacy- Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks vol. 14, no. 4, April 2015.

[4] Shu.T, Krunz.M, and Liu.S, "Secure data collection in wireless sensor networks using randomized dispersive routes". Vol. 9 no. 7, pp. 941–954, Mar 2010.

[5] Kennedy Edemacu, Martin Euku and Richard Ssekibuule "Packet drop attack detection techniques in wireless ad hoc networks: a review" International Journal of Network Security & its Applications (IJNSA), Vol. 6, No. 5, September 2014.

[6] Hridya V Devaraj, Asst. Prof. Jinu Mohan E_cient Technique for Privacy Preserving and Detection of Malicious Packet Dropping In Wireless Adhoc Networks(ICETEM-2016).

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

[8] Proano.A and Lazos.L "Packet-hiding methods for preventing selective jamming attacks" Dependable and Secure Computing., vol. 9, no. 1, pp. 101–114, Aug 2012.

[9] S. Buchegger and J.Y. L. Boudec, "Performance analysis of the confident protocol(cooperation of nodes: Faimess in dynamic adhoc networks),"in Proc.3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Cong.,2002,pp. 226-236.

[10] 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. 319333.

[11] 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. 135, 2008.