ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Detection of Packet Dropping Attack and Improving Detection Accuracy in Wireless Ad Hoc Network

[1] L. Leena Jenifer, [2] Y. Priyanka, [3] R. Ramya, [4] S. Sofia Kalaiarasi
[1] Assistant Professor, [2, 3, 4] IT Dept, Kings Engineering College, Chennai, India
[1] leenajeniferc87@gmail.com, [2] madhupriyanka31@gmail.com, [3] ramyaravi1095@gmail.com, [4] sofiakalai29@gmail.com

Abstract – The two main reasons for packet dropping in wireless Ad Hoc network are link error and malicious packet dropping. But we are not clear in identifying the correct reason for the packet loss i.e. whether it is due to link error or the combined effect of link error and malicious drop. We mainly focus on the malicious node packet dropping because due to the malicious dropping it drops selective packet dropping and which creates an ambiguous situation in the network. The older algorithms which are used to detect these malicious packet dropping does not provides satisfactory detection accuracy. Finding the correlation between the lost packets are used to improve the detection accuracy. The HLA (Homomorphic Linear Authenticator) mechanism is also used here to detect the truthful detection of packet loss in the wireless Ad Hoc network, because it is based on auditing mechanism were the auditor verifies the packet loss information reported by the nodes. This HLA also results in privacy preserving, collusion proof and incurs low communication and storage overhead, but has the disadvantage of this is HLA leads to computational overhead. To reduce thee computational overhead, we go for another concept called packet block based algorithm. By using all these methods we can improve the detection accuracy with low computation overhead.

Index Terms – privacy preserving, detecting attacks, Homomorphic Linear Authenticator, Auditor

I.INTRODUCTION

The station to station communication without access point is known as wireless Ad Hoc network. In the wireless Ad Hoc network there is packet loss occurs due to two reasons. One is due to link error i.e. the data is transferred via some nodes in the network, if any node in the network moves out of region, then the link in the network fails. Now the packet passed via the path will be dropped.

The second important reason is due to malicious nodes in the network [10]. Malicious nodes in the sense any node in the path which is attacked by the inside attacker to drop the packet. If any packet that transmits through the network, it is also dropped in the node itself.

To identify the reason for the packet loss, we first calculate the packet dropping rate. Based on the packet dropping rate we identify that is due to link error only or by the combination of link error and malicious nodes. But the impact of link error is ignored in this case. Therefore the packet dropping rate alone does not provide the true reason for the packet loss and the detection accuracy is less. Hence we develop an accurate algorithm for detecting the selective packet drop made by the inside attacker in the malicious nodes.

The high detection accuracy is obtained by calculating the correlation between the lost packets. ACF (Auto Correlation Function) is used to calculate the correlation between the lost packets. By using ACF we can decide the packet loss is due to the link error only or the combination of link error and the malicious nodes.

The packet loss bitmap is use to describe the status of the lost/received packets. But the great challenge in our method is packet loss bitmap reported by each and every node is not true. Because the attacker does not give the true information to the detection algorithms to avoid being detected. For example, the malicious nodes also knows about the packet loss bitmap and it drops the packet and informs that the packet has been forwarded. Here the truthfulness is avoided. These truthfulness is needed for the calculation of correlation of lost packets. Hence we go for an auditing mechanism which is used to verify the truthfulness of packet loss bitmap.

The solution for the above problem is given by using Homomorphic Linear Authenticator (HLA) [1] which is a signature based scheme. Anyway the direct application of the HLA does not perform well, because there is more than one malicious node in the network. These nodes exchanges the information during the time of attack and the time which they are asked to submit their reports.For example, a packet and its HLA signature needed to transmit from node 1 to node 2. That packet is dropped at node 1 itself and node 2 does not receive the packet. Since the node 2 is a malicious node, it sends back channel request to the node 1 and during auditing the node 2 provides a valid proof that it receives the packet. This is another drawback. Hence we go for **new HLA Construction.**

These new HLA construction has following features: **Privacy preserving:** [14]the auditor does not reveal the information that hoe it detect the malicious nodes.It incurs low communication and storage overhead. It reduces the computational overhead by introducing packet block based algorithm. The detection accuracy is also improved.

II.RELATED WORKS

Based on the packet dropping rate the are two scenario occurs. The first one aims at identifying all the malicious nodes in the network because most of the packet loss is due to malicious drop only. Here the impact of link error is ignored. There are three category in identifying the malicious nodes. The first category belongs to Credit system [2]. A node earns credits by sending all the packets it receives from the upstream node to the downstream node. The credit which earns will be very useful for the node for sending its own packet to the other nodes. In case of malicious nodes it continuously drops the packet it receives and loses the credits and does not able to transmits its own packet. The second method is reputation system [3]. The concept behind this reputation system is to identify the misbehaving nodes [11]. The bad reputation of any node is obtained due to the high packet dropping rate of that node. Due to the bad reputation the node loses the capability of sending the packets in the network. And also this malicious nodes is excluded from the path. The third method is hop to hop acknowledgementmethod [4], [5]. The hop with high packet loss is excluded from the network. The fourth method solves the problem occurs due to the cryptographic methods. The bloom filters is also used to identify the malicious nodes. Similarly another method called Renyi-Ulam game which traces the particular packet's route and the intermediator nodes. There is another condition that the first hop which does not transmit the packet for longer time is also considered as malicious nodes. Christo Ananth et al. [7] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

The second scenario is one in which the number of packet loss due to the malicious nodes is greater than the packet loss due to the link error, then the impact of link error is not ignored by having some knowledge in the wireless sensors. If the number of lost packet is greater than the expected packet loss due to link error, then there is high probability of packet loss is due to the malicious nodes.

All the above conventional methods does not give a satisfactory performance due to the following reasons: In credit system method, the malicious nodes receives the credit by forwarding most of the packet which receives from the other nodes. By using those credits, the malicious nodes also transmits the unwanted packets via the network. The second method called as reputation method, the malicious nodes maintains the good reputation by forwarding most of the packets it receives. Now the malicious node can able to transmit the packets. The bloom filters gives the proof for packet forwarding, and sometimes the proof was also wrong. In case of low packet dropping rate i.e. selective packet dropping case [12], the detection accuracy of Bloom filter is less. In the Hop to Hop acknowledgement method, the malicious nodes drops the packet it receives from the upstream node and sends an acknowledgement to the upstream node that it successfully transmits the packet.

Our proposed system aims to detect whether the packet loss is due to malicious error or link error. And to improve the detection accuracy by using packet block based algorithm and to reduce the computational overhead.

III.EXISTING SYSTEM

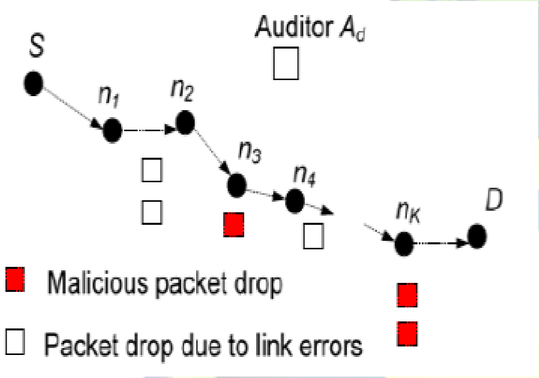


Fig.1 Packet dropping in the network

Let us consider the path between the source S and destination D as $P_{SD.}$ The source sends the packet to the destination D via the intermediatory nodes n1, n2,n3,……..,n_k. Where n1 is the upstream node of n2. For routing we uses the DSR (Dynamic Source Routing) [6], [8], [9] so the source have the knowledge of the path $P_{SD.}$ When we are not using the DSR, the source identifies the path by using trace routemechanism. In our method we focus on the static or quasi staticwireless ad hoc network, where the link and the network topology remains the same for a long time.

In the wireless model, the packet is transmitted in two states. I.e. good and the bad state, if the packet is successfully transmitted, then it is in good state, it is in bad state if the packet is lost.We does not use the Markovian property [15] and we uses the stationary distribution and Auto correlation function for finding the correlation between the lost packets. The link error statistics is Wide Sense Stationary (WSS).

As stated earlier, we consider only the static and quasi static wireless network, there we need to focus only on malicious nodes. Innon-static and high traffic network, there is always the node moves from one place to another, and it disturbs the causes of packet loss. There we mainly focus on the topology than the malicious nodes.

In HLA (Homomorphic Linear Authenticator),there is an auditor A_d is available to detect the malicious nodes. The auditor is not related to any node in the network and it is independent and it does not knows any information about the encryption mechanism, key etc. The main role of auditor is to detect the malicious nodes only. Consider that, the S sends packets to D, the D feels that something went wrong and report back to the S that the route is under attack [13]. This feedback is obtained due to loss of multiple packet of same type and performance drop. This feedback from Destination to Source is verified by the Source by using a cryptographic method called as Elliptic Curve Digital Signature Algorithm (ECDSA). Once the Source detects the attack, it sends ADR (Attack Detection Request) to the $A_{d..}$ The auditor verifies the truthfulness of packet by investigation method. All the nodes must give reply to the auditor‘s request. If the reply is received, then the node is considered as normal node and it can be able to send the packets along the network. If any reply is not received, then the auditor A_d identifies that node as malicious nodes.But sometimes the malicious nodes also cheats by sending the reply to the $A_{d.}$ Hence the truthfulness of detecting malicious nodes is avoided.

The network performance is reduced by malicious nodes are being undetected. Consider that the malicious nodes are aware of the algorithm used for detection of misbehavior nodes and it has the freedom to choose which packets it needs to drop. There are two types of packet dropping modes. They are i) Random drop mode ii) Selective mode. In random drop mode, the malicious node drop the packet with the probability $p_{d.}$ Where in selective mode, it drops the packets of particular type. Except the source and the destination any node in the network be malicious nodes in the path $P_{SD.}$The malicious nodes can exchange the information by using a convert communication channel. Using this channel the malicious nodes hides its misbehavior and reduce the chance of being detected. For example, the malicious node in the path P_{SD} drops a packet and secretly forwards the packet to the downstream node using the convert channel. When being investigated, the downstream node informs that, it receives the packet. This makes the auditor to believe that the packet was successfully forwarded to the downstream node and the malicious node is not detected in this case. Hence the truthful detection is avoided.

When a malicious node is detected, the auditor does not reveal the information about the malicious nodes. That information is kept private. This is known as privacy preserving.

Disadvantages:

i) The impact of link error is ignored

ii)Just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. This problem has not been well addressed in the existing system.

iii)Knowledge of the wireless channel is necessary

iv)The conventional algorithms used for detecting malicious nodes are not effective.

v)The truthfulness in detecting malicious nodes is avoided. Hence the detection accuracy is less.

IV. PROPOSED SYSTEM

i).Overview

To overcome all the drawbacks in the existing system, the correlation between the lost packets is identified. This is done by using ACF (Auto Correlation Function). The correlation between the lost packets shown in the diagram.

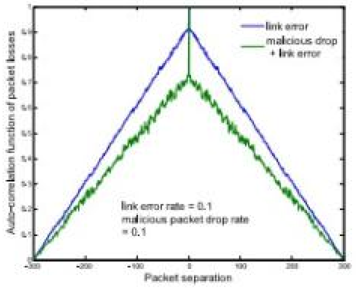
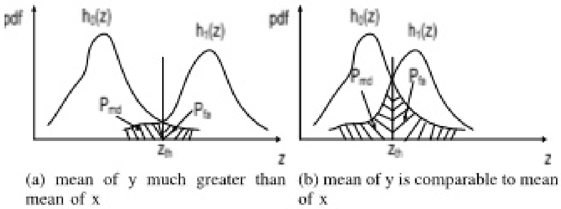


Fig.2comparison of correlation between the lost packets

If the packet dropping in the malicious nodes are selective, then it is inefficient in finding the correlation between the lost packets. Hence the detection in malicious nodes is also not accurate. This is shown in the following diagram.



(a) mean of y much greater than mean of x
(b) mean of y is comparable to mean of x

Fig. 3. Insufficiency of conventional detection algorithms when malicious packet drops are highly selective.

To improve the detection accuracy a new HLA method is constructed. In this new HLA construction, the source has to create the HLA key and the HLA signature for all the messages it transmits. This new HLA construction is used to detect the correct reason for the packet loss.

ii)Four Phases

a) Setup phase

The setup phase is established after the path P_{SD} is discovered but before the packet transmission takes place. The encryption decryption of the data packets occurs in this phase only. RSA algorithm is used to encrypt the packets. The source informs about the HLA key, signature and hash function to all the nodes in the path P_{SD}.

b)Packet Transmission Phase

After the setup phase, the packets are transmitted over the path $P_{SD.}$

c) Audit phase

In audit phase, the auditor receives the ADR(Attack Detection Request) from the source.By seeing the ADR the Auditor investigates all the nodes in the path $P_{SD.}$

d) Detection Phase

After receiving the reply from all the nodes, the auditor is now responsible for detecting the malicious nodes in the network. A normal node always replies with the correct information and the malicious nodes does not gives the original information. Those malicious nodes will be detected by the ACF. Once the malicious node is detected, it will be excluded from the path. Sometimes the feedback from the neighborhood nodes is received and the malicious node is detected and excluded from the node. After the detecting he malicious node, the information about how it detects the malicious node is kept secret. Hence it is privacy preserving.

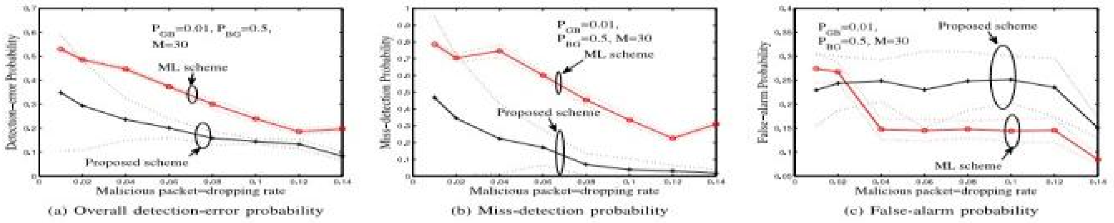
iii) Overhead Analysis

The computation in the new HLA is high when compared to the old conventional algorithms. The computation is done at the source node and it is high when compared to the other methods. The communication overhead is occurs when the path is established. In case of storage overhead the encryption and decryption key requires 56 bits. The hash function needs 160 bits because of using SHA algorithm. The HLA signature is also 160 bits long. To store all the values, we need 320+56 bits. Hence the storage is also less when compared to the old methods.

To reduce the computation overhead, we go for Block Based HLA signature method. In this method a block consists of more than one packets. Instead of calculating the HLA signature for each packet, the HLA signature is calculated for each block in the path by the source node.The auditing is also based on blocks. This will reduce the computation overhead of the new HLA method.

V) PERFORMANCE ANALYSIS

The two modes of packet dropping are Random packet dropping and malicious packet dropping

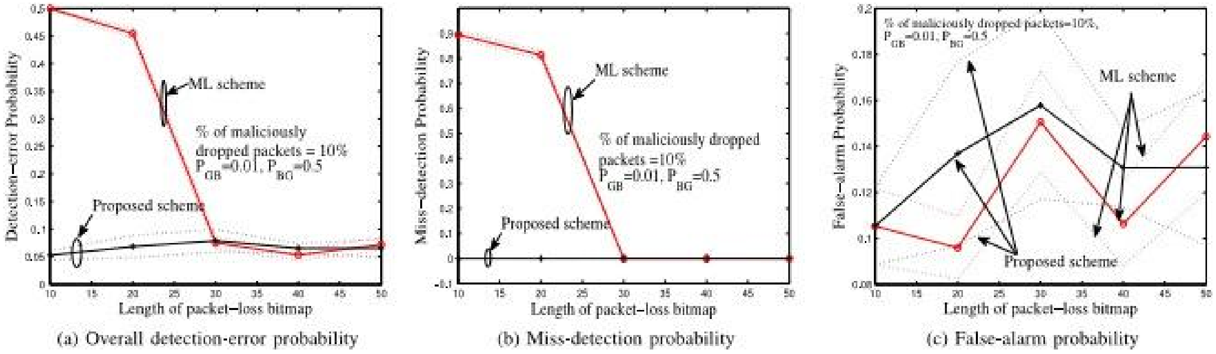


(a) Overall detection-error probability (b) Miss-detection probability (c) False-alarm probability

Fig.4. Random packet dropping.

The detection accuracy improved in the proposed scheme in case of random packet dropping, when compared to the conventional methods. It is shown in the fig.4.

The selective packet dropping detection accuracy is also improved as shown in fig.5.



(a) Overall detection-error probability (b) Miss-detection probability (c) False-alarm probability

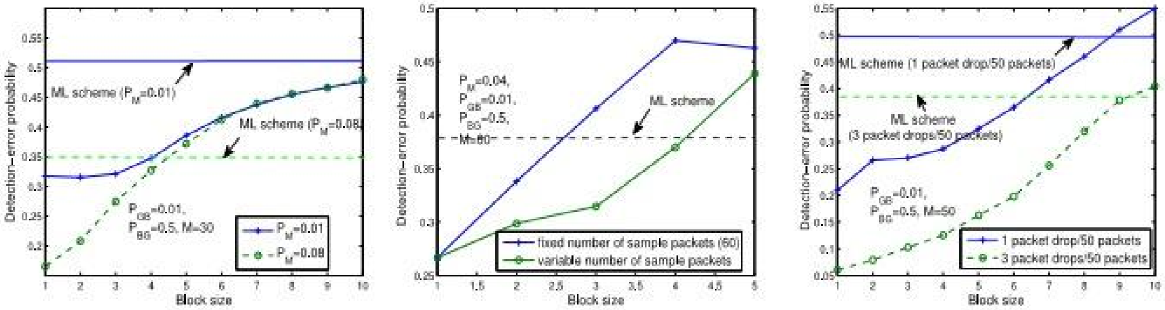
Fig. 5. Selective packet dropping evaluation

In case ofblock based detection the detection accuracy is improved as follows and it is shown in fig.6.

Advantages:i)The correct reason for the packet loss is identified. i.e. due to link error or combined effect of link error and malicious nodes.

ii)Detection accuracy is improved.

iii) The computation overhead is reduced by using block based algorithm.



(a) Random packet drops

(b) Impact of sample packets (random packet drops)

(c) Selective packet drops

Fig.6. Detection accuracy of block based algorithm.

VI) CONCLUSION

In this paper the reason for the packet dropping attacks in the wireless Ad Hoc network is identified. The HLA auditing architecture is introduced to detect the correct reason for the packet loss. To reduce the computation overhead in the HLA mechanism a new method called Block Based detection algorithm is used. The information about the malicious nodes detected by the auditor is kept private and the truthful detection of packet loss is achieved.

VII) REFERENCES

[1] 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. 319–333.

[2] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE INFOCOM Conf., 2003, pp. 1987–1997.

[3]Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830

[4] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

[5]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.

[6] 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. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[7] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[8]W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[9] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad

hoc networks," in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[10] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom Conf., 2000, pp. 255–265.

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

[13] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193

[14] T. Shu, S. Liu, and M. Krunz, "Secure data collection in wireless sensor networks using randomized dispersive routes," in Proc. IEEE INFOCOM Conf., 2009, pp. 2846–285

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

[16] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless net- works that are not bandwidth limited," in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.

[17] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Dec. 2008, pp. 90– 107

[18] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad-hoc routing service in adversarial environments," Wireless Pers. Commun, Special Issue Secur. Next Generation Commun., vol. 29, no. 3, pp. 367– 388, 2004

[19] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010

[20] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput, vol. 9, no. 1, pp. 101–114, Jan. Feb.2012.