Research Article

Detecting Truthfulness of Packet Dropping Attacks in WANETs

Sanma S Shetty[1]

Abstract: In multi-hop wireless ad hoc network packet loss can be caused mainly because of two different reasons. Link error and malicious packet dropping are two different reasons because of which packet losses can take place. Packet loss can take place because of link errors only, or by the combined effect of link errors and malicious drop. The accurate cause for the packet loss should be discovered. Here we are giving the consideration to insider attack case. In the insider attack case, i.e. the malicious packet dropping, malicious nodes will drop a small amount of packets which will affect the network performance. Based on traditional algorithms, it detects the packet loss rate does not attain adequate detection accuracy. To improve the detection accuracy, the correlations between lost packets is identified by using the bitmap obtained from individual nodes. By doing this exact reason for packet drop can be determined. The information reported by nodes should be truthful so, an public auditing architecture called Homomorphic linear authenticator (HLA) is developed. This architecture is privacy preserving and causes low communication and storage overheads. The auditor will collect the information reported by individual nodes and will determine the reason for packet loss by determining correlation between lost packets. Once the malicious node is identified the malicious node is eliminated from the route.

Asian Journal of Engineering and Technology Innovation
Volume 4, Issue 7
Published on: 7/05/2016

Cite this article as: Sanma S Shetty, Detecting Truthfulness of Packet Dropping Attacks in WANETs. Asian Journal of Engineering and Technology Innovation, Vol 4(7): 83-86, 2016.

INTRODUCTION

WANETs are used in networks which do not depend on a predefined network infrastructure. The environment were WANETs are used has no use of centralized administration and demands a dynamic network configuration. Since all the nodes in WANETs are portable it is mobile and so the topology is dynamic in nature. The nodes will not transmit the packets if there is any link failure or malicious drop. The transmission of data over the network is done by the nodes. If any one of the node fails in the network it will effect the network performance and the difficulty arises in setting up the routing table. "Figure 1," shows the small structure of wireless ad hoc networks.

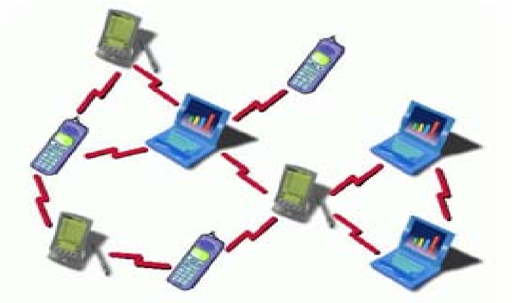

Figure 1: Wireless adhoc networks

In multi-hop wireless networks packet drop can occur because of link failure or malicious drop. There are two kinds of dropping. The first one is persistent dropping which means almost all the packets are dropped by the malicious node which it has received from the upstream node. This will completely degrade the performance of the network. It is easy to find these kind of malicious nodes. The second type of dropping is selective dropping, here the malicious node will drop the packets which is only of high importance. These kind of malicious nodes are difficult to identify. Here the chances of malicious nodes getting detected are lesser than that of the persistent dropping. So, detecting selective packet dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty arises because we need not only determine the place where packet drop has taken place but also determine whether the packet drop is intentional or unintentional. Intentional packet drop is because of the attackers and unintentional packet drop is because of hash channel conditions i.e. link failure. An acknowledgement based approach was used to determine the routing misbehavior and to overcome the adverse affect, as in [1]. This approach will identify the misbehaving nodes but does not determine the reason for packet drop. An identification scheme called REAct was proposed to determine the misbehaving nodes based on the proofs provided by individual nodes. Proofs are constructed by using Bloom Filters which are storage efficient structures, as in [2]. Even though the Bloom Filters provides proofs, it may contain errors.

[1] Reva Institute of Technology and Management, Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Near Border Security Bustop, Bengaluru, Karnataka-560064, India.
E-mail: ashwin@revainstitution.org
*Corresponding author

This paper proposes an appropriate algorithm for determining selective packet drop made by inside attackers. Once the malicious node is identified it is eliminated from the route so that it will not affect in future. Here the detection accuracy is high because we are finding the correlation between lost packets. The correlation between lost packets can be obtained by using the bitmap reported by individual nodes. Every node in the route will have a database which contains information regarding the reception status of packets, based on this a bitmap is created. By finding the correlation between lost packets we can determine whether the loss of packet is only because of ink failure or because of combined effect of link failure and malicious drop. The information provided by individual nodes should be truthful inorder to calculate the correlation between lost packets correctly. So an public auditing architecture called Homomorphic Linear authenticator (HLA) is developed. This mechanism is privacy preserving and provides low communication and storage overheads.

RELATED WORK

The existing system can be classified into two categories. In the first category almost all the packets are dropped because of malicious drop. Here the link error case is neglected. The first category is sub divided into four sub categories. These four sub categories will use four systems. These systems will work as follows:

Credit Systems

In this system, nodes will get credits for receiving and forwarding the packets to other nodes. The node can use the credit for forwarding its own packets. The credit of the malicious node will get reduced as it drops the packet and it will not be able to send its own packets, as in [3].

Reputation Systems

The Reputation system will depend on the neighboring nodes to monitor and identify the misbehaving nodes. If the node drops the packet it is given a bad reputation and if it does not drop the packet it is given a good reputation. The reputation information is periodically sent throughout the network to select the future route. If there is a malicious not it is eliminated from the route, as in [4].

End to End or Hop to Hop Acknowledgements

In this system end-to end or hop-to-hop acknowledgements are used to identify the malicious nodes. The hop were the packet drop is high is eliminated from the route, as in [1].

Cryptographic Methods

In this kind of system, misbehaving node is identified based on the proof provided by individual nodes. Proofs are constructed by using Bloom Filters which are storage efficient structures, as in [2].

The second category has high malicious packet drops than compared to link failure. In this case effect of link failure is not neglected. Here the traffic rate from the source and the traffic rate from the destination is compared. If the difference between these two rates are higher, then the packet drop is because of malicious drop and if the difference rate is low then the packet drop is because of link failure.

SYSTEM MODELS AND PROBLEEM STATEMENT

Network and Channel Model

The “Figure 2,” shows the routing path PSD. The source node S sends packet to the destination D through various intermediate node. The sender node knows the routing path by using Dynamic Source Routing Algorithm [DSR].

The autocorrelation function of the channel is fc (i) is the time lag of packets. Sequence of packets is transmitted from the sender through the channel. In order to verify the packets are transmitted or not the receiver will maintain a record such as {a1………..am} Where ajΣ {0, 1} j =1………..M. 1 represents packet was transmitted 0 represents packet discarded. fc(i) is derived by fc(i) = E { aj aj+1} for I =0,…………..M . ACF represents packet transmitted is received or lost at different time. There is an auditor in the routing path of the nodes. It does not have any knowledge about secret of the nodes. Auditor is used to detect the malicious node when it receives ADR request from the source. Source receives feedback from the destination. The integrity and authenticity of D is verified by the algorithm elliptic curve digital signature algorithm. Ad requires information from the node. I f any node was not replying correctly it is determined to be the malicious node.

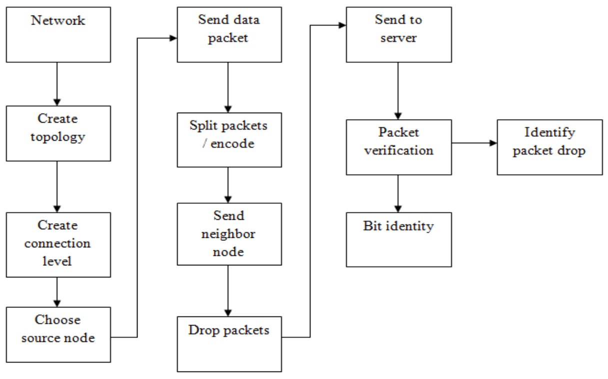

Figure 2: Architecture diagram

Adverserial Model

The goal of the adversary is to degrade the network's performance by maliciously dropping packets while remaining undetected. We assume that the malicious node has knowledge of the wireless channel, and is aware of the algorithm used for misbehavior detection. It has the freedom to choose what packets to drop. We assume that any node on PSD can be a malicious node, except the source and the destination. We consider the following form of collusion between malicious nodes: A covert communication channel may exist between any two malicious nodes, in addition to the path connecting them on PSD. As a result, malicious nodes can exchange any information without being detected by Ad or any other nodes in PSD. Malicious nodes can take advantage of this covert channel to hide their misbehavior and reduce the chance of being detected. For example, an upstream malicious node may drop a packet on PSD, but may secretly send this packet to a downstream malicious node via the covert channel. When being investigated, the downstream malicious node can provide a proof of the successful reception of the packet. This makes the auditor believe that the packet was successfully forwarded to the downstream nodes, and not know that the packet was actually dropped by an upstream attacker.

Under the system and adversary models defined above, we address the problem of identifying the nodes on PSD that drop packets maliciously. We require the detection to be performed by a public auditor that does not have knowledge of the secrets held by the nodes on PSD. When a malicious node is identified, the auditor should be able to construct a publicly verifiable proof of the misbehavior of that node. The construction of such a proof should be privacy preserving, i.e., it does not reveal the original information that is transmitted on PSD. In addition, the detection mechanism should incur low communication and storage overheads, so that it can be applied to a wide variety of wireless networks

PROPOSED WORK

In this paper we develop an appropriate algorithm for selective packet dropping made by inside attackers. The algorithm provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by finding the correlations between lost packets. The correlation is determined using the auto-correlation function (ACF). It will determine the packet loss bitmap describing the lost or received status of each packet. By detecting the lost packet we can determine whether the packet loss is due to link failure or combined effect of link failure and malicious drop.

The main challenge of the mechanism is to guarantee the packet loss bit maps reported by individual nodes are truthful. This truthfulness is important to calculate the correlation between lost packets correctly. This can be achieved by using an public auditor. This auditor is constructed based on Homomorphic linear authenticator (HLA) cryptographic primitive which is a signature scheme. The auditor will store the information reported by the individual nodes. "Fig. 3," shows the architecture diagram for the truthful detection of packet drop.

Initially the network is configured using the node configure function. The topology is created by selecting the number of nodes. The network topology is created by creating a link between source node, intermediate node and the destination node. The server is considered as the destination node and any one of the node is considered as source node. After creating the topology, in the source node the file is browsed which has to be sent. The file is split into packets. The split packets are then encrypted before transmission. The encryption is done based on RSA using the public key so that anyone can encrypt the packets. The encrypted packets are sent to the next intermediate node. If the intermediate node is not malicious node then it will forward all the encrypted packets to next node. If the intermediate node is malicious node then it will drop the packet. After the packets are been transferred it will reach the destination node. In the destination node packet verification is performed. Here we will get to know the malicious node and the number of packets dropped by it. The packets are decrypted at the destination node to view the contents of the file. The decryption process takes place using the private key. If malicious node is detected it is eliminated from the route.

The system consists of following phases:

Setup Phase

The network is configured here. The server is set as the destination node and any one of the node is considered as the source node. A network is created by connecting nodes with one another. The sender node is called as the upstream node and the receiver node is called as the downstream node. An arbitrary path PSD is created. Here s is the source and d is the destination. The packets are sent from source will go through the intermediate node and will reach the destination. "Fig. 3," shows the arbitrary path from source to destination. If there are any malicious node in between then it may drop the packets.

Packet Transmission Phase

After creating the path Psd from source to destination packet transmission takes place. Before transmitting the packets from the source node the packets should be encrypted. This encryption is based on RSA. Public key is used for encryption because anyone can encrypt the packet. The source node should also generate the HLA signature for each packet. So, the packet is transferred from the source along with its HLA signature. The next receiving node will store this packet and the HLA signature in the database as a proof of reception and the transmission process continues. Each node will create a bitmap. 1 indicates packet has been received successfully and 0 indicates there has been a packet drop. Based on the bitmap created correlation between lost packets is calculated.

Independent Auditor

The auditor is independent because it is not associated with any node and the auditor will not be having any information regarding the packet contents. The auditor is constructed based on HLA. Every node along the route will have the database which contains proof of reception status. After sending all the packets when the destination node reports that the route is under attack to the source node, the source node will send attack detection request (ADR) to the auditor. When the auditor receives this ADR request it performs auditing to determine the truthfulness of packet drop. The auditor will now challenge each node. The normal node will reply with the correct information and the malicious node may cheat. So, for the truthful detection we are using HLA architecture.

Packet Drop Detection

Whenever the verify button on the destination node is clicked the packet drop detection is performed. The packet drop detection is performed by using correlation between lost packets. By doing this we can determine the malicious node. The HLA construction is privacy preserving because the auditor will not be able to vie the contents of the packet. After the packet transmission in the destination node we will get to know the place where packet loss has been taken place and the reason for the packet drop. Once the malicious node is detected it is eliminates from the route. So, in future transmission that particular malicious node will not effect the packet transmission process.

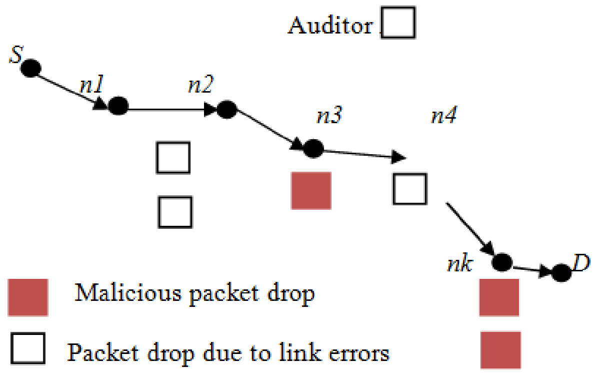

Figure 3: Packet drop because of link failure and malicious drop

EXPECTED RESULTS

In proposed mechanism once the malicious node is determined it is eliminated from the route. Most of the computation for generating HLA signature is done at the source node and for conducting detection the work is done by the auditor. So, this will reduce computational overhead. The storage overhead is also less. The proposed mechanism provides high detection accuracy. It is also privacy preserving because the auditor will not be knowing about the contents of the packet. It will receive only the information reported by individual nodes.

CONCLUSION AND FUTURE WORK

Conventional algorithm detects the packet loss but it does not achieve satisfactory detection accuracy. To improve the detection accuracy correlation between lost packets is determined. The high detection accuracy is achieved by identifying the correlations between the positions of lost packets and it is calculated using auto-correlation function (ACF) of the packet loss bitmap. So by determining the correlation between lost packets we can determine whether the packet loss is because of link failure or malicious drop. To correctly calculate the truthful packet loss information HLA based public auditing architecture is developed. This will ensure the truthful packet loss information reported by individual nodes. This architecture is collusion proof and it requires high computational capacity at source node. It will incur low communication and storage overheads over the route.

For the future work we can use different methods to generate keys for the generation of signatures to reduce the overhead and we can use some encryption method to obtain the data confidentiality. Extension to dynamic environment will be studied in future work.

REFERENCES AND NOTES

1. 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.
2. W. Kozma Jr., and L. Lazos, “REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proc. ACM Conf. Wireless Netw. Secur.,2009, pp. 103–110.
3. 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.
4. 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.