Various attacks and its detection techniques in packet dropping in wireless ad hoc network

Priti Mesare[1], Dr. S. S. Sherekar [2], Dr. V. M. Thakare [3]
PG. Department of ME Computer Science and information technology, SGBAU, Amravati.
Email: mesarepriti@gmail.com[1] , ss_sherekar@rediffmail.com[2], vithakare@yahoo.com[3]

Abstract- In wireless ad hoc network several computing devices are connected with each other through RF and not having fixed infrastructure and centralised control and the network packets are send from source node to destination node. Communication between multiple nodes is takes place with the help of multi hop wireless links, during the communication of one node with other then number of packet are loss leads to link error or malicious packet dropping. for detection of packet dropping attack the audit based misbehaviour detection, audit based misbehaviour detection and monitoring, truthful detection, side channel monitoring techniques are used. It consists, comparisons of various existing techniques and analysed the various attack and its detection techniques in packet dropping, and its challenges. This paper focuses on a novel framework for packet dropping attack in wireless ad hoc network.

Index Terms-— packet dropping; secure routing; attack detection; misbehaviour;

1. INTRODUCTION

Wireless ad- hoc network is decentralized type of ad hoc network. The network is ad hoc because it does not rely on pre-existing infrastructure, such as route in wired network or access point in managed wireless network. Wireless ad hoc network are self configuring, dynamic network in which nodes are free to move and so the determination of which node forward data is made dynamically based on network connectivity. Although wireless ad hoc network hold promise for a large application in different domain and are expected to the revolutionize in everyday life, the problem of Securing this network from various different attacks.
One of the most dangerous attack in wireless ad hoc network is packet dropping attack class of denial of service attack, where the attacker attempt to stop the normal use of resources or service temporally, indefinitely or permanently. Packets are drop because of collision, overflow of transmission queue, broken link due to nodes, error in packet mobility and lack of energy resource.

DETECTION OF PACKET DROPPING ATTACK IN WORELESS AD HOC NETWORK

There are five detection techniques study and analysed in this paper, in wireless ad hoc network packets sends from source to destination.

(1) Link error and malicious packet dropping are two sources of packet losses in multi hop wireless ad hoc network. As shown in fig 1. Packets drop owning to malicious packet drop and link error.

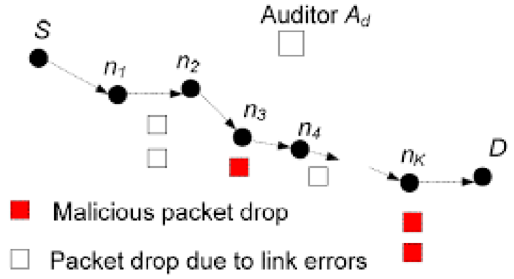

FIG1: NETWORK AND ATTACK MODEL

In this sequence of packet are losses to detect whether the packet losses due to link error or malicious drop truthful detection technique is used.

(2) Packet drop attack targeting at message forwarding service in network environment by dropping packet maliciously if the attacker drops packet in bulk then another effective detection technique used that is side channel monitoring.

(3) To make a secure packet delivery in multi ad hoc network and identify the misbehaving nodes and eliminating them from packet transmission the effective technique that is audit misbehaviour detection and monitoring method.
(4) The black hole attack is a dangerous attack which adversary nodes try to drop all or partial received packet instead of forwarding them to next hop, to defend network from this attack dynamic trust model is used.
(5) The problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi hop ad hoc network the technique which is used Audit based misbehaviour detection.

2. BACKGROUD

In wireless ad hoc network, node cooperate in relaying or routing traffic An adversary may exploit this nature to launch attacks and the adversary starts dropping packets. In the most severe form, malicious nodes simply stop forwarding every packet, the various techniques are used to detect the behaviour of nodes, link error and malicious dropping are two sources of packet losses, in this to detect whether the losses caused by link error or malicious drop, homomorphic linear authenticator (HLA) based public auditing allows the detector to verify truthfulness of packet drop information [1]. Another detection techniques acknowledgement to prove that node was actually forwarded packets to the next hop, the receiver can send acknowledgement in the reverse direction for multiple hops. However, it fails when more than two malicious node are colluding in a row. For example, three malicious node one next to another act as a tem to drop packets along a communication path: the one in middle actually drop packet , while its prior hop simply does not do drop packets, while its prior hop does not do watch dog job and its next hop falsely send acknowledgement [2].

Acknowledgement based system relay on the reception of acknowledgements to verify that a message was forwarded to next hop, this scheme is called TWOACK, where the node send two hop acknowledgement message along the reverse path verifying that intermediate node faithfully forwarded packets. Packets that have not acknowledgement remain in cache until they expire. A value is assigned to the quality of un-verified packet to determine misbehaviour. ACK based system also incur a high communication and energy overhead for behavioural monitoring. For each packet transmitted by source, several acknowledge must be transmitted and received over several hops. Moreover they cannot detect attacks of selective nature over encrypted over end to end flow , to overcome this the audit based misbehaving detection technique can detect selective dropping attack even end to end traffic is encrypted and can be applied to multi channel network consisting of node with directional antennas[3].

The advance technique that is audit based misbehaving detection and monitoring method, effectively monitor both continuous and selective packet droppers to forward packet through the reputed nodes [4].

The authentication mechanism, based on message authentication code (MAC) and pseudo random function (PRF) for detecting black hole attack, now the dynamic trust management system proposed to detect black hole attack. [5].

The rest of this paper is organized as follows: **Introduction** gives packet dropping attack in wireless ad hoc network in S**ection 1**. **Background** gives a premise of the proposed research problem is pointed out, and then the proposed problem is formalized in detail in **Section 2**.**Previous Work done** gives related work of the current approaches improving detection methods of packet dropping will be introduced briefly in **Section 3**. **Existing methodology** discussed in **Section 4.** Analysis and Discussion discuss In **Section 5. Proposed methodology** gives the design and implementation process of the proposed method is introduced in detail and **Possible Result** discussed in **Section 6.** Finally, **Conclusion** of the paper discussed in **Section 7**.

3. PREVIOUS WORK DONE

S.Zong, et al. (2003) [1], In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four subcategories. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

S. Kurosawa, et al. (2007), [2] identify packet drop attackers during routing process so as to prevent the attacks from happening. Watchdog method as a special case. Unlike Watchdog which is ineffective to cooperative attacks, SCM is able to detect attackers acting as a team. Unlike the version of Watchdog [A. patcha] extended to cooperative attacks.

S. Buchegger, et al. (2005), [3], identifying misbehaving nodes either use some form of per-packet evaluation of peer behaviour or provide cooperation incentives to stimulate participation. Incentive-based approaches do not address the case of malicious nodes who aim at disrupting the overall network operation. L. Buttyan, On the other hand, per-packet behaviour evaluation techniques are based on either transmission overhearing or issuance of per-packet acknowledgements.

Crowcroft R et al., (2003) [4], proposed a scheme that adjusts the credit reward to traffic and congestion conditions. While credit-based systems motivate selfish nodes to cooperate in the packet transmission, but they do not provide any incentive to malicious nodes in the network.. Such nodes have no intended to collect credit for forwarding their own traffic.

J. Luo, M, et al. (2008), [5], proposed an authentication mechanism, based on the message authentication code (*MAC*) and pseudo random function (*PRF*) for detecting black hole attack. A game theoretic approach for identifying the black hole attack

4. EXISTING METHODOLOGY

Packet dropping techniques are truthful detection, side channel monitoring, audit based misbehaviour detection, audit based misbehaviour detection and monitoring, dynamic trust model.

Truthful detection: Detection of packet dropping attack and proposed homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. HLA does not solve problems well because of problem set up by users. It results detection accuracy is improved in random packet dropping and selective packet dropping case [1].

Side channel monitoring: The attacks are performed by compromised intermediate nodes, either alone or cooperatively, in an already established data communication path. The proposed detection technique, named *Side Channel Monitoring (SCM)*, which has the well-known Watchdog method. SCM results to detect attackers acting as a team. SCM does not require trusted nodes (thus no additional hardware investment) and involves only local communication (thus more efficient)[2].

Audit based misbehaviour detection: The system ADM identify and isolate the misbehaving nodes that refuse to forward the packets. AMD system integrates reputation management, trustworthy route discovery and can detect selective dropping attack even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas [3].

Audit based misbehaviour detection and monitoring: AMDMM provide the paths consist of highly reputed nodes, subject to a desired path. When paths contain misbehaving nodes, the proposed monitoring system effectively audits and enhances the nodes reputation for the proper communication. The identification strategy obtains through knowledge of nodes' reputation. Also, this monitoring method performs the reputation using storage-efficient membership structures. It results The AMDMM recovers the network operation even if a large fraction of nodes misbehaving at a significantly lower communication cost [4].

Dynamic trust model: Defending packet dropping attack and proposed Dynamic trust model to defend network against attack, In this approach, all nodes in the network trust together initially. By getting feedback from the network, nodes may update the trust value related to their neighbours. When trust value of a neighbour is less than a predefined threshold; a suspicious node will be identified as an adversary [5].

5. ANALYSIS AND DISSCUSSION

Truthful detection in which homomorphic linear authentication technique is used for detection of packet dropping attack is best suited for condition to verify the truthfulness of packet loss information reported by node due to which the detection accuracy increases. 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. Privacy-preserving: the public auditor should not be able to discern the content of a packet delivered on the route through the auditing information submitted by individual hops. 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. [1].

Side channel monitoring (SCM) technique to detect packet drop attack in ad hoc networks SCM use two channels: primary channel and side channel. The set of nodes adjacent to the each node in the active route for communication will be selected as observer to monitor the message forwarding misbehaviour. Nodes of active route are part of primary channel and observer nodes are part of side channel. After detecting misbehaviour, the monitor nodes inform the source node by sending alarm message through both the channels. . SCM is able to detect the cooperative attacks and involves local communication only. But there is no encryption technique to secure the channels. Also, nodes performing partial dropping are undetectable. [2].

Audit based misbehaviour detection system for detecting and isolating misbehaving nodes. AMD can operate in multi-channel networks and in networks with directional antennas. Current packet Overhearing techniques are only applicable when transmissions can be overhead by peers operating on the same frequency band. AMD detects selective dropping behaviours by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end-to-end traffic is encrypted. [3].

The advance audit technique audit misbehaving detection and monitoring method for safe and secure packet delivery that also effectively monitor both continuous and selective packet droppers to forward packet through the reputed nodes. [4].

The dynamic trust model is best suited for defending packet drooping in which the black hole attack try to attract all the packets on network and then drop them , the dynamic trust model increase packet delivery ratio and trust degree of neighbour node.[5]

5.1. Advantage and disadvantages of the methods are discussed as shown in Table1.

Method/ Algorithm Used	**Advantages**	**Disadvantages**
Homomorphic linear authenticator	1. Detection error decreases with probability of message (PM). 2. The overall detection error probability of proposed scheme is lower than Malicious Link (ML) scheme. 3. Detection error probability under correlated packet losses is in general smaller than uncorrelated packet loss.	Conventional algorithms detecting packet loss rate cannot achieve satisfactory detection accuracy. .
Side channel monitoring	1. SCM performed effective detection of abnormal node which drops packets. 2. SCM is effective in various network scenarios.	Low performance rate in some scenario. .
Dynamic trust model	1. All the adversary nodes are detected by proposed algorithm. 2. Dynamic trust model increases Packet delivery ratio and increase the	The proposed algorithm detects some normal node as adversary. .

	trust degree of neighbour node.	
Audit based misbehaviour detection	1. AMD successfully avoid misbehaving nodes, even when large portion of network refused to forward packet. 2. AMD can operate in multi-channel networks and in network with Directional antennas. .	Sometimes the large portion of network refuses to forward packet.
Audit based misbehaviour and monitoring method	1. AMDMM successfully avoid misbehaving nodes. 2. AMDMM can operate in multi-channel networks and in network with directional antennas. 3. AMDMM effectively monitor both selective and continuous packet droppers to forward packet through reputed node. .	Sometimes the large portion of network refuses to forward packet.

Table 1. Advantages and disadvantage

5.2. Performance Attributes for packet dropping attack in wireless ad hoc network

Various performance attributes and properties considered in existing packet dropping techniques in wireless ad hoc network are discussed below:

- Throughput: The throughput is the time interval ratio between packets received to the packet sent. In other way, per-node throughput is the average time of the number of bits transmitted by each node to its destination. The sum of per-node throughput over all the nodes in a network is called the throughput of the network. For the packet dropping detection technique throughput decides detection accuracy so that it should be high.
- Acknowledgement: the node has received packet and forward the packet to next hope and the acknowledgement from hop shows successful packet transmission , acknowledgement improve accuracy and detect similar fault so that this parameter should be increased.
- Timeliness: Regular update in the routing is needed to be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of the links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information. If a node that relays information between two large connected components is advertised as "down" by malicious neighbours, large parts of the network become unreachable.

6. PROPOSED MEHODOLOGY

The proposed packet dropping techniques which combined time based model and side channel monitoring which detects the compromised nodes for false detection. These two models run together. Malicious nodes on the path can give the wrong impression about the time-based module by providing incorrect information. To prevent this problem, side channel monitoring detects attackers acting as a team. SCM monitor message forwarding behaviour of node, on observing misbehaviour, they issues alarm packet to the source node.

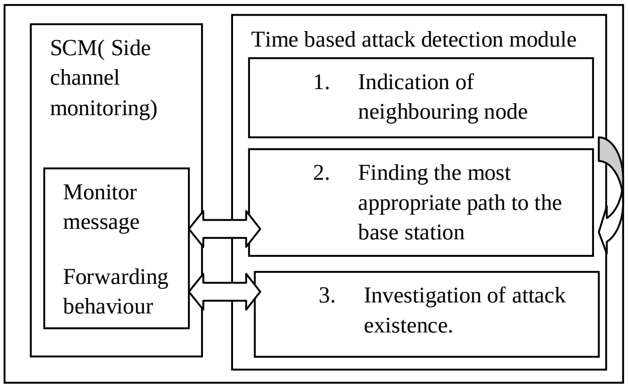
SCM(Side channel monitoring)
Monitor message
Forwarding behaviour
Time based attack detection module
1. Indication of neighbouring node
2. Finding the most appropriate path to the base station
3. Investigation of attack existence.

Fig: The SCM with time based attack detection module.

time based module indicate neighbouring node and find most appropriate path to base station but malicious node on the path can gives wrong impression about time based module to avoid this side channel monitoring technique available to monitor message forwarding behaviour of nodes and also avoid replay attack by forwarding valid information in particular interval of time. Finally time based attack detection module investigate existence of attack and find most appropriate path, it improve detection accuracy.

6.1. POSSIBLE OUTCOME AND RESULTS

The goal of this research was to determine whether the literature on detection of packet dropping techniques in wireless ad hoc network provides a uniform and rigorous base and this research is to establish best security against packet dropping attack and control various attack to forward safe packets.

The proposed framework shows side channel monitoring method and time based attack detection module combination which is effective to control various attacks such as replay attack, delay attack by monitoring malicious node, message forwarding behaviour and time based module find one trusted path for message forwarding. These two modules effectively combines and support to avoid packet dropping attack. The expected results presented here thus give a attacks detection accuracy of the existing detection techniques in wireless ad hoc network.

7. CONCLUSION

Wireless Ad Hoc Network With the increased number of lightweight devices as well as evolution in wireless communication, the ad hoc networking technology is gaining effort with the increasing number of widespread applications. The various packet dropping attack detection techniques are analysed in Wireless Ad Hoc Network. In proposed framework side channel monitoring model basically monitor malicious node and message forwarding behaviour which helps time based module to provide valid information in specific time interval. This technique is effective for sending message on best path in specific time interval. In today's world security is most important and it is essential for protecting various information such as business related and personal information.

FUTURE SCOPE

This paper proposed a packet dropping attack detection techniques and secure this technique using cryptography as well evaluates its performance through simulation.

REFERENCES

[1]Tao Shu and Marwan Krunz, Fellow, IEEE **"**Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks" , IEEE TRANSACTIONS ON MOBILE COMPUTING. VOL. 14, Issue NO. 4, pp 813-828- APRIL 2015.

[2] Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks", IEEE ICC international conference on communication, 11year 2011.

[3] Yu Zhang, Loukas Lazos, Member, IEEE, and William Jr. Kozma. "AMD:Audit-Based Misbehaviour Detection in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 8, pp1893-1907- AUGUST 2016.

[4] Vijayakumar.Aa*, Selvamani Kb*, Pradeep kumar Aryac," Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks,". ELSEVIER procedia computer science. VOL. 48, pp485-495- 2015

[5] Mohammad Taqi Soleimani, Mahboubeh Kahvand, "Defending Packet Dropping Attacks Based on Dynamic Trust Model in Wireless Ad Hoc Networks" ,Mediterranean electro technical conference. Vol. 13, pp362-366- 16 April 2014.