INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING
VOL. 1 ISSUE 3, DEC.-2012 ISSN NO: 2319-7463

PTSNN & PIMN: Packet Testing the Sincerity of Neighbouring Nodes and Packet Informing for Malicious Nodes in Ad Hoc Networks

Hussain Saad Alshahrani[1], Prakash Veeraraghavan[2]
Department of Computer Science and Engineering, Latrobe University, Melbourne, Australia.
[1]hsalshahrani@gmail.com

Abstract: Malicious nodes are hard to detect and can easily affect other nodes in the network. These malicious nodes can attack other nodes by changing information, sending incorrect information or retaining information and not sending on to other nodes. Moreover, these nodes may cooperate with other malicious nodes in other networks to achieve their aims. In this paper, we present an algorithm for detecting and isolating malicious nodes from the network. Our algorithms introduce two new mechanisms which are **Packet Testing the Sincerity of Neighbouring Nodes (PTSNN) and Packet Informing for Malicious Nodes (PIMN)**. These mechanisms assist legitimate nodes to detect and isolate malicious nodes in their network. Moreover, these mechanisms deal with the **certificate Authority (CA)** which can issue and revoke certificates for nodes. In addition, if any node is detected and isolated by the PTSNN and PIMN, the certificate of this node is revoked and recorded in **Certificate Revocation List (CRL)** which contains all the revoked certificates.

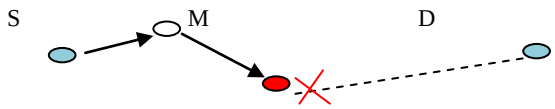
Keywords: Malicious nodes, certificate authority (CA), certificate revocation list (CRL), PTSNN and PIMN.

1. Introduction

Ad hoc networks are considered one of the most important types of wireless networks. Therefore, a large body of research has been dedicated to these types of networks. It is most important that these networks are secure, reliable and trustworthy. Moreover, in ad hoc networks, the nodes communicate with each other without wires or central access points. In these types of networks, there are two types of protocols: the proactive routing protocol which assists in passing on up-to-date routing information from one node to the other nodes in the network; and the reactive routing protocol which calculates the route to the destination. When the route is created, the source can communicate and send data to its destination [2]. The most popular routing protocol used is the ad hoc on-demand distance vector (AODV). This protocol has two types of packets, a route request (RREQ) and a route reply (RREP). When the source node wants to send a packet to the destination where the route is not available, it broadcasts the RREQ. If the destination receives the RREQ, it uncasts the RREP to the source [1] [3]. The second important protocol is dynamic-destination sequenced distance victor (DSDV).This protocol is regarded as a proactive routing protocol. In this protocol, each node has to set tables to store the routing information. Moreover, it uses the distance vector shortest path routing. This means that, if there are many paths to reach the destination, it will select the shortest one [1] [2]. In this case, they may face many attacks from other nodes called malicious nodes. These illegitimate nodes can affect the other legitimate nodes by changing information or sending incorrect information. Moreover, these nodes may cooperate with other malicious nodes in other networks to attack other nodes to achieve their aims. Therefore, these nodes have to be detected and isolated from networks.

2. Malicious nodes

It is well known that any network contains many nodes. These nodes can communicate after they authenticate each other and they can transmit and exchange data between them. In other words, they have to have trust between them to communicate. However, some nodes, which are a part of the network and have been trusted, may be malicious nodes. These nodes can affect the network and its own members by propagating many attacks in this network such as changing information. Moreover, these nodes may cooperate with other legitimate nodes to achieve their aims. Sometimes, these nodes send incorrect information to other nodes or may not forward the packets to other nodes in the network. In this case, the network suffers due to these nodes.



S = Source, D = Destination node, M = Malicious node.

Figure 1: Malicious node

For example: source node S wants to send a packet to destination node D. S sends the RREQ packet to discover a route to reach D and after a while, it receives the RREP packet from D. It is assumed that there are 100 hops (nodes) between S and D. All of these nodes forward the packet, and this packet has not been changed. As we have previous discussed that malicious nodes may cooperate with other legitimate nodes to achieve their aims. Therefore, any node from these 100 nodes could be a malicious node which may cost the network by disconnecting the communication. In other words, when S sends information to D, S does not know if D receives the information or not, D may not receive the information or it receives incorrect information, M may keep the information and send the RREP to S, when S receives the RREP, it thinks the packet came from D but in fact it came from M. Therefore, the information is lost. In this case, there should be a method to protect the network and its members from these malicious nodes. Therefore, we propose new methods which are the **Packet Testing the Sincerity of Neighbouring Nodes (PTSNN) and Packet Informing for Malicious Nodes (PIMN)**. These packets can detect and isolate the malicious nodes from the network. These packets will be discussed later.

3. Overview

In our algorithms, there are four main steps which have to be considered as follows:

Step 1: Any node should have authorization to join the network and communicate with the network's members. In other words, all nodes in the network possess certificates of authentication. In other words, a new node cannot join the network unless it possesses this certificate.

Step 2: All nodes in the network can communicate with each other after they have received the certificate of authentication. However, any node which wants to send a packet to another node must discover a route that can reach its destination.

Step 3: When a sender node knows its destination node, it sends the Packet Testing the Sincerity of Neighbouring Nodes (PTSNN) packet through the intermediate nodes until it reaches its destination. This packet is a test for nodes.

Step 4: If any node tries to change or drop the PTSNN packet, the previous trusted node sends PIMN packet to all its neighbours include the sender node to tell them about this malicious node. In this case, the certificate of this node is revoked and recorded in the certificate revocation lists (CRLs). Therefore, this node cannot join the network anymore and cannot communicate with other nodes in the network, as in the past.

4. Packet Testing the Sincerity of Neighbouring Nodes (PTSNN)

This packet assists to detect and Isolate the malicious nodes from the network. This packet has these fields:-

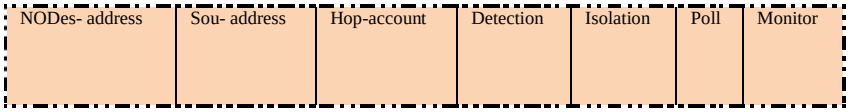


Figure 2: Packet Testing the Sincerity of Neighbouring Nodes (PTSNN)

Destination address field: can assist the packet to reach the destination node.

Source address field: can assist the packet to return to the source node

Hop account field: can assist to account for the nodes. It uses the original hop account which is received by the RREP packet.

Detection field: collects information from other nodes. This information includes the status of each node and how it works. Therefore, any node which either tries to change the packet or does not forward the packet will be known as a malicious node. Moreover, this field contains three fields inside it which are node-IP-address, node-hop-account, and flag. See figure 3:

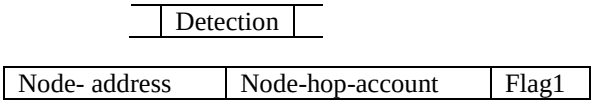


Figure 3: Detection field.

- Node- address: this field records the node addresses which receive the PTSNN packet.
- Node-hop-account: this field contains the hop number of the nodes which receive the PTSNN packet.
- Flag1: there are two hop account fields in the PTSNN packet. The first one is the original hop-account which contains a constant value. This value comes from the hop account in the original RREP packet which has been sent from the destination to the source. However, this value cannot be changed, except in one case which is, if the detection field finds any node which tries to change or does not forward the packet, this value will be changed to (0) instead of the original value. The second is the node-hop-account which was explained in the previous point. The flag1 field uses these two fields to detect if the node is malicious or not. If the flag1 field is greater than or equal to (0), this node will be a trusted node. Otherwise, this node is a malicious node. This field works as follows:

  - We assume that hop-account from the RREP is = 100.
  - We assume that node-hop-account is = 80.
  - If the node works very well, the flag1 field cannot change the original hop-account.
  - Flag1 = ((hop-account value) - (node-hop-account value)).

    = (100 - 80).

    = 20 > 0

  - Trusted node.

Node- address	80	20

  - If the node tries to change or does not forward the packet, the flag1 field changes the original hop-account to (0).
  - Flag1 = (0 - 80).

    = - 80 < 0

  - Malicious node.

Node- address	80	-80

Isolation field: this field deals with flag1 from the detection field. Moreover, this field contains two fields which are next-hop and flag2. The flag2 field contains one of these two values "+1" or "-1". The "+1" value means that the node has not been isolated. The "-1" value means that the node has been isolated. The next-hop field depends on the flag2 field. If the flag2 is "+1", the node-hop-account will increase by 1. Therefore, the PTSNN packet will be sent to the next node. But if the flag2 is "-1", the node-hop-account will not increase. See figure (4). Therefore, this node will be isolated from itself. This field works as follows:

Isolation	

Flag2	Next-hop

Figure 4: Isolation field.

> If flag1 > = 0 e.g. 20 > 0
> Flag2 = "+1"
> Next-hop = node-hop-account + 1

Node- address	80	20	"+1"	81

> Else flag1 < 0 e.g. -80 < 0
> Flag2 = "-1"
> Next-hop = node-hop-account

> Copy these two fields and put them in the PTSNN of the malicious node.

Node- address	80	-80	"-1"	80

Poll field: this field has the default value "TRUSTED". This field deals with flag2 in the isolation field. If the value of flag2 is "+1", the poll field takes the default value "TRUSTED". When the value of flag2 is "-1", the poll field changes its value to "UNTRUSTED". See figure 5:

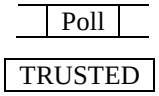


Figure 5: Poll field.

> If flag2 = "+1"
> TRUSTED

Node-address	80	20	"+1"	81	TRUSTED

> If flag2 = "-1"
> UNTRUSTED

Node-address	80	-80	"-1"	80	UNTRUSTED

Monitor field: this field is responsible for forwarding the packet to the next node or sending it back to the previous node. Moreover, this field deals with three fields: two from the isolation field which are flag2 and next-hop and the third field is poll field. This field works as follows:

> If ((flag2 = "+1")
> And (next-hop = node-hop-account + 1)
〉 And (poll = "TRUSTED"))
⇒ The packet is forwarded to the next node.

> If ((flag2 = "-1")
> And (next-hop = node-hop-account)
〉 And (poll = "UNTRUSTED"))
⇒ The packet will not be sent to any node.

However, the malicious nodes may change these information and send it to the next node. In this case, the PIMN packet runs.

5. Packet Informing for Malicious Nodes (PIMN)

This packet contains these two fields:

Figure 6: PIMN packet

Node address: it is a malicious node address.

Node certificate: it is the certificate that is issued when the node joins the network.

Operation:

This mechanism runs in every node in the network. When the PTSNN packet has been sent to the next node and this node tries to change the packet's data, the previous node sends a PIMN packet to all neighbours to inform them of this malicious node. When each node receives this packet, it records the node address and certificate in the certificate revocation list (CRL). In this case, this malicious node is revoked from the network and cannot join it again. Therefore, this packet is considered as an informer.

6. Algorithm

Our network is distributed to clusters. Each cluster contains the following nodes: CA node, gateway node, warranty node and regular node plus a new node that wants to join the network. Every node has a public/ private key which is generated by the node itself. The public key assists the node to obtain a trusted certificate to join the network. The CA node is the head of each cluster in the network and is responsible for issuing and revoking the certificates. Each cluster communicates with other clusters through gateway nodes. There are some trusted nodes, called warranty nodes, which can assist the CA to make a decision about a new node. However, there may be malicious nodes in the network which have the authorization to communicate with all members in the network. The malicious nodes in the network may try to launch an attack by modifying a message before forwarding it or they may not forward the message at all. We try to detect these nodes and isolate them from the network and try to rediscover a new route to reach the destination. Therefore, the proposed algorithm for the detection and isolation of the malicious nodes is focused on route discovery, authentication, and the proposed solution which is the PTSNN packet.

I. Route discovery

The source node sends the RREQ (which contains <source-add, source-seq-num, broadcast-id, destination-add, destination-seq-num, hop-cnt>) to its own neighbours to discover the route to the destination node. Each node receives the RREQ and records the address of the neighbour which is received by the RREQ. Once it has done that, the reverse route from this node to the neighbours, back to the source is set up. Moreover, the RREQ contains two sequence numbers which are: source sequence number which assists the node to maintain information about the reverse route to the source, and destination sequence number which assists the node to maintain information about the route to the destination. The route entries of the reverse path are kept for a sufficient period of time to traverse the network and create a RREP to the source. When the intermediate node which has a current route to the destination receives the RREQ, it compares the destination sequence number in its route entry with the destination sequence number in the RREQ. Therefore, if the destination sequence number in the route entry is greater than or equal to that in the RREQ, this node can reply and it unicasts the RREP to its neighbour from which it received the RREQ. Otherwise, this node rebroadcasts the RREQ. However, any node may receive the same RREQ twice from various neighbours in which case the latest RREQ will be dropped. See figure 7:

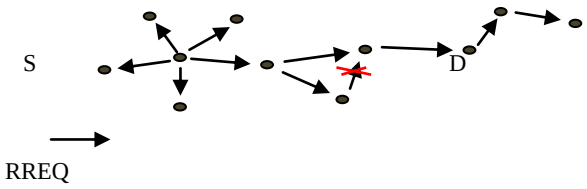


Figure 7: The route request

Now the reverse route has been created from the destination to the source. Therefore, the destination unicasts the RREP (which contains <source-add, destination-add, destination-seq-num, hop-cnt, lifetime>) to the source. When the RREP travels to the source by the reverse route, each node along this route has to: set up the forward pointer to the node from which the RREP came; update its timeout information for route entries to the source and destination; and record the latest destination sequence number for the requested destination. Therefore, the nodes which are not along the path and are not determined by the RREP will timeout after 3000 msec and the reverse pointers will be deleted. If further RREPs are received, it updates the routing information. If the new RREP contains a greater des-seq-num than the previous RREP or the same des-seq-num with a smaller hop count, it propagates. As soon as the source receives the first RREP, it can begin data transmission, and it can update its routing information when it learns of a better route. See figure 8:

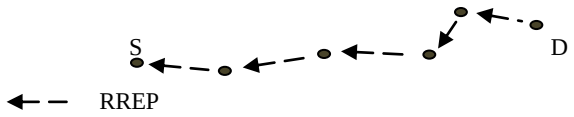


Figure 8: The route replay

There is what is called **Timer-to-Trust**. The TTT contains a specific period of time. If the source node does not receive the RREP during this time, the route is dropped.

Now the source node knows the route to reach its destination. However, any node from the intermediate nodes may be a malicious node which cooperates with other nodes to achieve its purpose. Therefore, a new mechanism is introduced which is Packet Testing the Sincerity of Neighbouring Nodes (PTSNN), which contains the following fields: Des-address, Sou-address, Hop-cnt, Detection, Isolation, Poll, and Monitor. These are discussed in the next section.

II. PTSNN and PIMN algorithms

This algorithm can be used to detect and isolate malicious nodes from a set of nodes and can be used in different clusters. Each cluster can come up with information about the malicious nodes which have been detected and isolated by the PTSNN packet. As mentioned in the previous section, the PTSNN packet contains seven fields: 1) the destination address field which is used for discovering where the destination is, so the packet can reach the destination node by using the address of destination; 2) the source address field which assists the packet to return to the source node through the reverse route. As mentioned in the previous section, the source node sends the RREQ to find the route to the destination node. When the source node receives the RREP, it knows how many hops are between itself and its own destination. The RREQ packet and the RREP packet have hop account fields which give the same value. Therefore, 3) the hop account field in the PTSNN packet takes the same value of these fields which can assist in knowing how many nodes are between the source and destination. Moreover, this field assists the PTSNN packet to detect and isolate the malicious nodes; 4) the detection field which is responsible for detecting malicious nodes. Moreover, it collects information about each node, and it has three subfields which are; 1) the current node address field which contains the IP address of the current node; 2) the node hop account field which contains the number of the node which receives the PTSNN packet; 3) the flag1 field; and, as we have mentioned previously, the hop account field in the PTSNN packet, which has a value which cannot be changed unless a malicious node has been detected. In this case, the value of the hop account is changed to (0) by the monitor field. The flag1 field uses these two fields (hop account and node hop account) to determine whether the current node is a trusted node or a malicious node; 5) the isolation field, which deals with the flag1 subfield from the detection field and contains two subfields. The first subfield is the flag2 field which either takes "+1" value or "-1" value. In other words, if flag1 is positive, flag2 takes "+1"; if flag1 is negative, flag2 takes "-1". The second subfield is next hop. This field will increase by 1 if flag2's value is "+1"and it decreases by 1 if flag2's value is "-1". Moreover, there is another field which is called 6) the poll field. This field has a default value which is "TRUSTED". If the flag2 subfield has "+1" value, the poll field takes the default value "TRUSTED". But if the flag2 subfield has "-1" value, the poll field changes its value to "UNTRUSTED". The last field in the PTSNN packet is a 7) monitor field which is responsible for controlling the fields of packet. In this case, we have two assumptions that are discussed as follows:

- **First assumption**

In this assumption, we assume all nodes in the network are legitimate nodes. In this case, the PTSNN packet is forwarded till it reaches the destination node. When the destination node receives the packet, it copies the information from this packet and puts it in its own table and it exchanges the source address with the destination address. Therefore, the previous destination address becomes the source address and the previous source address becomes the destination address. Then, it sends the packet back to the source node through the reverse route. When the source node receives this packet back from the destination, it knows this route is secure and can be used for data transmission. See figure 9:

Figure 9: Data Transmission

- **Second assumption**

In this assumption, we assume there is a malicious node somewhere in the network. When this malicious node receives the PTSNN packet, this node may try to change the packet's information or may not forward the packet. In this case, the previous trusted node sends the PIMN packet to all neighbours. When all nodes receive the PIMN packet which contains the address and certificate of the malicious

node, these nodes revoke any connection with this node. In this case, the previous trusted node, which sends the PIMN packet, rebroadcasts RREQ to find a new route to the destination. Once it finds a new route to the destination, it sends the PTSNN packet again to reach the destination. See figure 10:

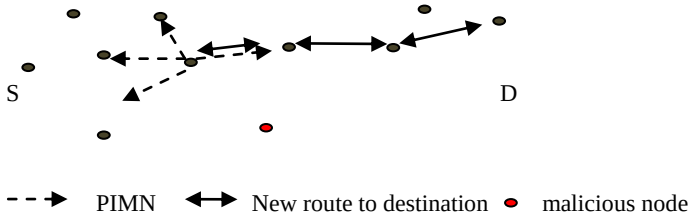


Figure 10: Detection and Isolation a malicious node

III. Authentication

A network contains many nodes. These nodes can communicate with each other. However, they have to authenticate each other before they communicate. In other words, they cannot communicate with each other unless they have authentication between each other. Therefore, if a node wants to join the network, it generates a public/ private key pair. Then, it sends CREQ to its own neighbours to obtain a certificate for authentication. When the CA, which is a responsible for issuing the certificates, receives this request, it sends the CA beacon to this node to ask it to identify itself and give warranties. In this case, this node sends a message to the other trusted nodes to get warranties from them. Once it has received the warranties, it sends a CREQ with its public key and the warranties to the CA. When the CA receives this packet, it issues a certificate for this node and sends it with the CA beacon to the node. When the node receives its certificate, it can communicate with other nodes and shares information with them. However, there may be one or more malicious nodes in the network which may affect the network by changing information or not forwarding it to other nodes. In this case, the PTSNN packet assists in detecting and isolating these nodes, as discussed in the previous section. When these nodes have been detected and isolated from the network, the CA revokes all the certificates of these nodes and records these certificates in the CRLs which contain all the revoked certificates. The CRLs are sent with the CA beacons by the CA to all the nodes in the network. In this case, when all the nodes receive these CRLs, they then know about the malicious nodes in the network. Therefore, the malicious nodes cannot cooperate with other nodes and the other nodes will not deal with these malicious nodes. As a result, the network security is increased.

Conclusion and future work

In this paper, we introduced two new mechanisms one is called Packet Testing the Sincerity of Neighbouring Nodes (PTSNN) and the second is called Packet Informing for Malicious Nodes (PIMN). These mechanisms can detect and isolate malicious nodes from the network. If any node tries to change information or does not forward the packet to other nodes, it is detected and isolated as a malicious node by the PTSNN and PIMN packets. In this case, this node cannot join the network and other nodes cannot communicate with it. Moreover, these packets deal with the CA and CRLs. The CA is responsible for issuing and revoking certificates of nodes, so it is in charge of the cluster of nodes. The CRLs contain all revoked certificates. Therefore, if the PTSNN and PIMN isolate a malicious node, the certificate of this node is recorded in the CRL. Consequently, these mechanisms can protect the network and its members from malicious nodes. However, they have some weaknesses such as time delay and overhead. In future, these weaknesses may be discussed and solved which can assist to improve these mechanisms.

References

[1]. A. Al-Mazyad, H. Al-jouir, “Simultaneous Multi-Routes QoS Routing for ad hoc Networks (SMRQR)”, IEEE Xplore, pp.685-694, 2008.

[2]. C. Kaufman. DASS, “Distributed authentication security service”, Request for Comments 1507, September 1993.

[3]. M. Gasser, A. Goldstein, C. Kaufman, B. Lampson, “The digital distributed systems security architecture”, In Proceedings of the 12th National Computer Security Conference, pages 305–319, Baltimore, MD USA, October 10–13, 1989.