International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
1793-8201

Detection and prevention of wormhole attack in mobile adhoc networks

Shalini Jain, Dr.Satbir Jain

Abstract—**Wireless networks are suspectible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. In such attacks two or more malicious colluding nodes create a higher-level virtual tunnel in the network, which is employed to transport packets between the tunnel endpoints. These tunnels emulate shorter links in the network and so act as benefit to unsuspecting network nodes which by default seek shorter routes. This paper present a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, we demonstrate that our scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.**

Index Terms—**Ad hoc networks, computer network security, computer networks, tunneling, wireless LAN, wormhole, packetleash.**

I. Introduction

An ad-hoc network is built, operated, and maintained by its constituent wireless nodes. These nodes generally have a limited transmission range and so each node seeks the assistance of its neighbouring nodes in forwarding packets . In order, to establish routes between nodes, which are farther than a single hop, specially configured routing protocol are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. The nodes in an ad-hoc network generally have limited battery power and so active routing protocols endeavor to save upon this, by discovering routes only when they are essentially required. In contrast, proactive routing protocols continuously establish and maintain routes, so as to avoid the latency that occurs during new route discoveries. Both types of routing protocols require persistent cooperative behaviour, with intermediate nodes primarily contributing to the route development. Similarly each node, which acts like a mobile router, has absolute control over the data that passes through it. In essence, the membership of any ad-hoc network indisputably calls for sustained benevolent behaviour by all participating nodes. In real life, such an altruistic attitude is more than often extremely difficult to realise and so we often find malicious nodes also present in the same network. Some of these are alien nodes, which enter the network during its establishment or operation phase, while others may originate indigenously by compromising an existing benevolent node. These malicious nodes can carry out both Passive and Active attacks against the network.

In passive attacks a malicious node only eavesdrop upon packet contents, while in active attacks it may imitate, drop or modify legitimate packets [14]. The severity of such attacks increases multifold especially when these are performed in collusion. A typical example of such a cooperative attack is a wormhole in which a malicious node tunnels the packets from one end of the network to another. The tunnel essentially emulates a shorter route through the network and so naive nodes prefer to use it rather than alternate longer routes. The advantage gained by the colluding nodes is obvious as they are now for all intents and purposes, in charge of a high usage route through the network. The consequences of such a wormhole on the network can be catastrophic, and in worst-case scenarios, may lead to a vertex cut in the network.

In this project, we apply a similar trust based scheme to the Dynamic Source Routing (DSR) protocol to detect and evade wormhole attacks in a pure ad-hoc network. Each node in the network autonomously executes the trust model and maintains its own evaluation regarding other nodes in the network.

This paper is divided into total of six sections. Section 1 consists of introduction, Problem statement and problem definition. Section 2 describes the basics of Routing and vulnerability found in today's Adhoc networks. Section 3 is the security issues in wireless Adhoc networks followed by previous work done on wormhole attack in next section. Section- 5 is about DSR and its working. Section 6 consists of approach and methodology for detecting and evading wormhole. Section 7 depicts design and implementation and section 8 gives simulation results of our proposed trust based model. Section 9 concludes with the conclusion and future work.

A. Problem Statement

The increasing popularity and usage of wireless technology is creating a need for more secure wireless

Manuscript received September 20, 2009.

Shalini Jain is Lecturer with the Maharaja Surajmal Institute of Technology, Affilated with Idraprashta University, New Delhi, India (phone:+91-9873099411; fax: 91-11-25528116; e-mail: shallu.jainr@gmail.com).

Dr. Satbir Jain is an Asst .Prof with Delhi University (Netaji Subash Institute Of Technology,) in Computer Science Department, New Delhi, India. (e-mail:Jain_Satbir@yahoo.com).

networks. Wireless networks are particularly vulnerable to a Powerful attack known as the wormhole attack [10] [1]. This paper disscuses a new trust based that prevents wormhole attacks on a wireless network. A few existing Protocols detect wormhole attacks but they require highly specialized equipment not found on most wireless devices. This project aims to develop a defense against Wormhole attacks that does not require as a significant amount of specialized equipment.

B. Problem Definition

Ad-hoc or spontaneous wireless networks are threatened by a powerful attack known as the wormhole attack. A wormhole attack [10] [1] can be set up with relative ease, but preventing one is difficult. To set up a wormhole attack, an attacker places two or more transceivers at different locations on a wireless network as shown in figure1 as follows.

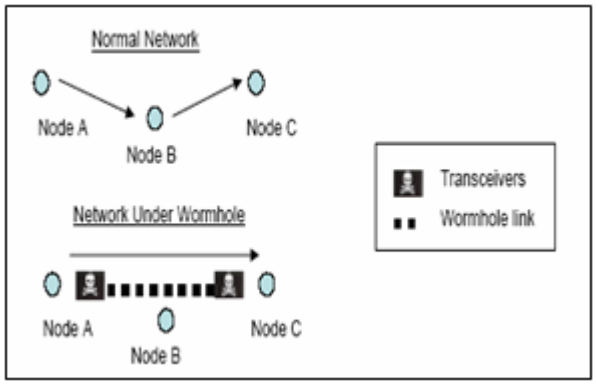

Figure1 Set-up of a wormhole.

Node A can reach node C within a shorter time with the help of a wormhole[16].
This establishes a wormhole or tunnel through which data can transfer faster than it could on the original network. After setting up a wormhole, an attacker can disrupt routing to direct packets through the wormhole using a technique known as selective forwarding[10] depicted in Figure 2.

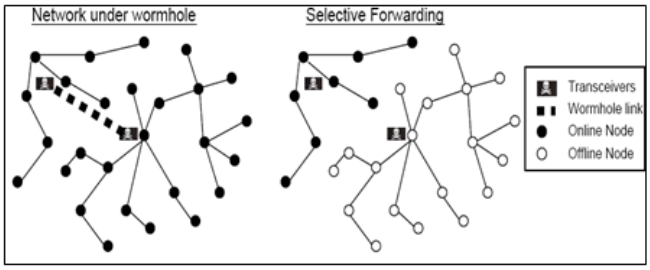

Figure2 Selective Forwarding.

Lower right portion of network relies on wormhole link to route information. Disconnecting wormhole link results in breakdown of the network[16].

A strategic placement of the wormhole can result in a significant Breakdown in communication across a wireless network. Wireless networking is a young technology and thus, many wireless network devices have not been designed to defend against wormhole attacks. For example, a sensor network device called the Mica mote has the ability to sense information about its surroundings such as temperature, sound or movement. The Mica mote has little room for security measures to protect itself from a wormhole attack. Current network protocols are also vulnerable to wormhole attacks. So its very necessary to find out an useful scheme for detection and evasion of wormhole. This paper will introduce a trust based model for same purpose.

II. ROUTING

The knowledge of routing protocols of MANETs is important to understand the security problems in MANETs. The routing procols used in MANETs are di-
erent from routing protocols of traditional wired world because of frequent route updates, mobility and limited transmission range. The performance criteria of nodes in MANETs are different than that of wired networks.

Routing protocols in Mobile Adhoc Networks are majorly of two categories: Proactive Protocols and Reactive Protocols

Reactive Routing protocols are based on corresponding routes between two nodes , when it is required. This is different from traditional *Proactive Routing* Protocols in which nodes periodically sends messages to each other in order to maintain routes.

Dynamic Source Routing(DSR) uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet . This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms: Route Discovery and Route Maintainance.

Route Discovery is used when the sender does not know the path upto the destination. In this mechanism, the sender broadcasts a ROUTE REQUEST message which contains Source Address, Destination Address , Identier. Each intermediate node adds its address in ROUTE REQUEST message and rebroadcast it, unless it has not rebroadcasted earlier. With this controlled broadcast, the ROUTE REQUEST will ultimately reaches the destination. The destination then sends a unicast ROUTE REPLY message in reverse direction whose information is obtained from list of intermediate nodes in ROUTE REQUEST message. When the ROUTE REPLY packet reaches the source, it records the route contained in it and saves in its cache for the specic destination. For better performance, intermediate nodes also records this route information from the two route messages. All nodes overhearing these packet adds meaningfull route entries in their caches.

Finally, Route Maintainance Mechanism is used to notify souce and potentially trigger new route discovery events when changes in the network topology invalidates a cached route.

III. SECURITY IN AD HOC NETWORKS

Due to the issues such as shared physical medium, lack of

IACSIT International Association of Computer Science and Information Technology WWW.IACSIT.ORG

central management, limited resources and highly dynamic topology, ad hoc networks are much more vulnerable to security attacks [4]. Hence it is very necessary to find security solutions. In the following sections we first address attacks in ad hoc networks, and list several typical special attacks.

we can classify the attacks into two brief categories, namely passive and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.Active attacks can be further classified into two types according to the location of attackers, namely internal and external active attacks. According to the layer attacked they can be classified into network layer attacks, transport layer attacks, Application layer attacks, and multi-Layer attacks.

1) *Network layer attacks*

Attacks which could occur in network layer of the network protocol stack are:-

Wormhole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point [10].This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

Black hole attack: In this attack, a malicious node attempts to suggest false path to the destination. An adversary could prevent the source from finding path to destination, or forward all messages through a certain node [10] [1].

Routing attacks: In this attack, an adversary attempts to disrupt the operation of the network. The attacks can be further classified into several types, namely routing table overflow attack, routing table poisoning attack, packet replication attack, route cache poisoning, and rushing attack. In a routing table overflow attack, an adversary attempts to cause an overflow in routing table by adverting routes to non-existent nodes, while in routing table positining attack the adversary sends false routing updates or modifies the actual routing updates to result jam in networks.

2) *Transport layer attacks*

Transport layer attacks is generally session hijacking. In this type of attack, an adversary obtains the control of a session between two parties. In most cases the authentication process is executed when a session begins, hence an adversary could take the role of one party in the whole session.

3) *Application layer attacks*

In this type of attack, an adversary analyzes the vulnerability. Dozens of attacks aiming at application layer exist, such as script attack, virus, and worm.

4) *Multi-Layer attacks*

Attacks, which could occur in any layer of the network protocol stack, fall into this class.

Spoofing attack: Spoofing attacks are also called impersonation attack. The adversary pretends to have the identity of another node in the network, thus receiving messages directed to the node it fakes. One of these attacks is man-in-the-middle attack. In this attack, attackers place their own node between two other nodes communicating with each other and forward the communication.

Denial of service attack: In this type of attack, the attacker attempts to prevent the authorized users from accessing the services. Due to the disadvantage of ad hoc networks, it is much easier to launch Dos attacks. For example, an adversary could disrupt the on-going transmissions on the wireless channel by employing jamming signals on the physical and MAC layers.

5) *Others*

Unlike above addressed attacks, in a device tampering attack, devices such as PDA could get stolen or damaged easily. The adversary could then get useful data from the stolen devices and communication on behalf of the owner.

IV. Background Work

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks[6]. Directional antennas are able to detect the angle of arrival of a signal . In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east). This protocol fails only if the attacker strategically placed wormholes residing between two directional antennas.

Another localization scheme known as the coordinate system involves the work done by **Nagpal, Shrobe and Bachrach** at Massachusetts Institute of Technology (MIT). It uses a subset of GPS nodes to provide nodes without GPS a sense of relative location . This is achieved using two algorithms:The gradient which measures a GPS node's hop count from a point in a network, and multilateration, which determines the way GPS nodes spread information of its location to nodes without GPS. Hop counts tell how far a node is from a particular source. A flaw in using this scheme is that wormholes can disrupt hop counts within a network . Therefore, any system following this scheme is rendered defenseless under wormhole attacks.

Rouba El Kaissi et.al[21]obstacles impede the successful deployment of sensor networks. In addition to the limited resources issue, security is a major concern especially for applications such as home security monitoring, military, and battle field applications. This paper presents a defense mechanism against wormhole attacks in wireless sensor networks. Specifically, a simple routing tree protocol is proposed

Y. C. Hu et.al.[18] have considered packet leashes – geographic and temporal. In geographic leashes, node location information is used to bound the distance a packet can traverse. Since wormhole attacks can affect localization, the location information must be obtained via an out-of-band mechanism such as GPS. Further, the "legal" distance a

packet can traverse is not always easy to determine. In temporal leashes, extremely accurate globally synchronized clocks are used to bound the propagation time of packets that could be hard to obtain particularly in low-cost sensor hardware. Even when available, such timing analysis may not be able to detect cut-through or physical layer wormhole attacks.

In **S. Capkun et.al.[19]**, an authenticated distance bounding technique called MAD is used. The approach is similar to packet leashes at a high level, but does not require location information or clock synchronization. But it still suffers from other limitations of the packet leashes technique. In the Echo protocol [20], ultrasound is used to bound the distance for a secure location verification. Use of ultrasound instead of RF signals as before helps in relaxing the timing requirements; but needs an additional hardware. In a recent work [4], authors have focused on practical methods of detecting wormholes. This technique uses timing constraints and authentication to verify whether a node is a true neighbor. The authors develop a protocol that can be implemented in 802.11 capable hardware with minor modifications. Still it remains unclear how realistic such timing analysis could be in low-cost sensor hardware.

In this paper, the performance of multi-path routing under wormhole attack is studied in detail by Ning Song et.al[22]. They showed that multi-path routing is vulnerable to wormhole attacks. A simple scheme based on statistical analysis (called SAM) is proposed to detect such attacks and to identify malicious nodes. Comparing to the previous approaches (for example, using packet leash), no special requirements (such as time synchronization or GPS) are needed in the proposed scheme. Simulation results demonstrate that SAM successfully detects wormhole attacks and locates the malicious nodes in networks with different topologies and with different node transmission range.

V. Wormhole Attack In DSR

In any ad-hoc network, a wormhole can be created through the following three ways:

- Tunneling of packets above the network layer
- Long-range tunnel using high power transmitters
- Tunnel creation via external wired infrastructure

In the first type of wormhole, all packets which are received by a malicious node are duly modified, encapsulated in a higher layer protocol and dispatched to the colluding node using the services of the network nodes. These encapsulated packets traverse the network in the regular manner until they reach the collaborating node The recipient malicious node, extracts the original packet, makes the requisite modifications and sends them to the intended destination.

In the second and third type of wormholes, the packets are modified and encapsulated in a similar manner. However, instead of being dispatched through the network nodes, they are sent using a point to-point specialized link between the colluding nodes. In this thesis, we only discuss solutions to the first type of wormhole, which in our opinion has greater applicability to pure ad-hoc networks. In an ad-hoc network executing the DSR protocol, each packet contains the complete list of nodes that it has to traverse in order to reach the destination. This feature, although excludes intermediate nodes form making any routing decisions, can still be exploited to create a wormhole. Such wormholes can be created in a number of topological scenarios.

However, all such settings are primarily derived from scenarios where the colluding nodes (M1,M2) are not the immediate neighbours of the source (S) and destination (D) nodes.Wormhole creation in such a scenario is generally accomplished using the following steps:

Sustained Routes between Colluding Nodes M1 and M2 periodically establish and maintain routes to each other in the network at all times. This route serves as a higher layer tunnel for all other nodes whose traffic is routed through M1 and M2.

Fallacious Response to Source Node Route Requests whenever a ROUTE REQUEST packet from S is received by M1, it immediately sends a ROUTE REPLY packet so as to portray minimal delay. M1 also makes the ROUTE REPLY packet (S-1-M1-M2-D) as short as possible, indicating D as an immediate neighbour of M2. Such ROUTE REPLY packets, have a high probability of being selected by S as they have minimal hop-count and latency.

*Route Development till the Destination Node*M1 informs M2 to initiate a route discovery to D through a pre agreed upon higher layer protocol and also performs the same. In the mean time, all data packets from S to D are buffered for a certain interval at M1. While waiting for a route to D, if M1 receives a ROUTE REPLY packet from D to S, it verifies whether it can reach D through M2. If yes, it creates a new working source route option from M2 to D (S-M1-M2-5-D) for the buffered packets, encapsulates and sends them to M2, else it waits for the ROUTE REPLY packet to be received in response to the ROUTE REQUEST packet that was initiated by itself and M2.

Upon receipt of these ROUTE REPLY packets, M1 traces an optimal route to D through M2. However, if during this waiting period, the buffer interval expires or an overflow occurs, M1 sends a ROUTE ERROR packet to S for the last received data packet.

IACSIT International Association of Computer Science and Information Technology WWW.IACSIT.ORG

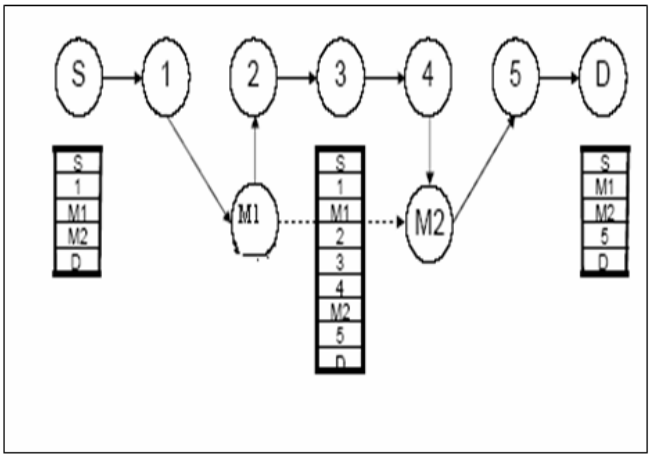

Figure3 Wormhole attack in DSR

Deception through Gratuitous Route Replies As an alternate mechanism, if M1 overhears any ongoing communication between S and D (S-1-2-3-4-5-D). It may initiate a new route discovery to D and also request the same through M2. Upon receipt of a route from M1 to D via M2, it can create a new Gratuitous ROUTE REPLY packet (S-1-M1-M2-D) and send it to S. Based upon the same criterion for route selections may classify the newly received route as optimal and discard the one that was already in use.

VI. Approach and Methodology

Main goal is to design a protocol that not only prevents wormhole attacks but also Avoids using strict clock synchronization, limits the need for specialized equipment, ensures information confidentiality,provides high performance, low power consumption and minimal memory storage.

A. Trust Model

We detect and evade wormholes in the network using an *effort-return based trust model*. The trust model uses the inherent features of the Dynamic Source Routing (DSR) protocol to derive and compute respective trust levels in other nodes. For correct execution of the model, the following conditions must be met by all participating nodes:

1 All nodes support promiscuous mode operation.

2 Node transceivers are omnidirectional and that they can receive and transmit in all directions

3 The transmission and reception ranges of the transceivers are comparable.

Each node executing the trust model, measures the accuracy and sincerity of the immediate neighbouring nodes by monitoring their participation in the packet forwarding mechanism. The sending node verifies the different fields in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust counter is incremented. Similarly, if the integrity checks fail or the forwarding node does not transmit the packet at all, its corresponding direct trust measure is decremented. We represent the direct trust in a node y by node x as Txy and is given by the following equation:

$$Txy = PP \cdot PA \quad (1)$$

Where PP e [0, 1], represents the situational trust category Packet Precision, which essentially indicates the existence or absence of a wormhole through node y [14]. PA represents the situational trust category Packet Acknowledgements that preserves a count of the number of packets that have been forwarded by a node. The category PP and PA are employed in combination to protect the DSR protocol against wormhole attacks and for identifying selfish node behaviour respectively. Any benevolent node not able to forward a data packet, due to radio interference, hardware faults, software bugs or environmental conditions, is classified as selfish. However, in case no other alternate trusted nodes are available, these selfish nodes will be engaged into the routing process.

However, any node incorrectly forwarding a data packet, by not ensuring its integrity, will be classified as malicious and not included in any subsequent data connections.

B. Wormhole Detection

During wormhole detection, each node in the network measures the accuracy and sincerity of its immediate neighbouring nodes. The detection process works in the following manner:

1 Each node, before transmission of a data packet, buffers the DSR Source Route header. After transmitting the packet, the node places its wireless interface into the promiscuous mode for the Trust Update Interval (TUI). The TUI fundamentally represents the time a sending node must wait after transmitting a packet until the time it overhears the retransmission by its neighbour. This interval is critically related to the mobility and traffic of the network and needs to be set accordingly. If this interval is made too small it may result in ignoring of the retransmissions, similarly a large value may induce errors due to nodes moving out of range.

2 If during the TUI, the node is able to overhear its immediate node retransmit the same packet, the sending node increases the situational trust category PA for that neighbour. It then verifies whether the retransmitted packet's DSR Source Route header is the same as the one that was buffered earlier. If this integrity check passes, the situational trust category PP is not set, indicating an absence of a wormhole. However, if the retransmitting node modifies the DSR Source Route header, the detecting node sets PP to true.

3 In case no retransmission is heard and a timeout occurs when the TUI has exceeded, the situational trust category PA for that neighbour is reduced and the DSR Source Route buffer is cleared. With the passage of time, the number of inter-node interactions also increase, increasing each node's knowledge of the behaviour of other nodes.

Any forwarding node, which had earlier detected wormhole creation by any of its immediate neighbour, drops

all packets that were destined to go through that neighbour and generates a corresponding ROUTE ERROR packet. This packet informs the source and all intermediate nodes regarding the unavailability of the route through the wormhole. Consequently, the wormhole is circumvented in subsequent data connections.

C. *Wormhole Evasion*

In DSR, before initiating a new route discovery, the cache is first scanned for a working route to the destination[8]. In the event of unavailability of a route from the cache, the ROUTE REQUEST packet is propagated. When the search is made for a route in the cache, the Dijkstra algorithm is executed, which returns the shortest path in terms of number of hops. In the LINK CACHE scheme the default cost of each link is one, which signifies uniform spread of the inter-node trust levels. We replace this cost with the actual trust level of a node to which this particular link is directed. Now, each time a new route is required, a modified variant of the search algorithm is executed, which finds routes with the maximum trust level. However, before cost assignment to any link, each node first checks the wormhole status of the link end node. If it has been classified as a wormhole, the cost of that link is set to infinity. This method ensures that wormholes nodes are avoided in all future data connections.

VII. Design & Implementation

Here we introduce the trust value mechanism by incorporating trust formation and trust updating as solution to the vulnerability of the DSR protocol.

1 For each node in the network, a trust value will be stored that express the trust for these nodes. This trust value will be adjusted based on experiences that a node has with other its neighbour nodes.

2 When a packet received data packets or acknowledgements the trust value for this node will be updated.node that is encountered for first time will has an initial trust value assigned based on some trust formatting strategy.

3 If the requested acknowledgement was not received, the trust value for this node should be decreased.

4 The selection of best route will be based on some scenarios that use the trust values of the nodes on the route.In figure:4 we illustrate the design diagram of Trusted DSR

A. *Modified DSR Protocol Design*

*Trust Formatter Module:*When new mobile nodes encounter in the network Trust formatter component implements methods to assign trust values to these nodes. An initial trust value will be assigned to the new nodes when first route is discovered because all nodes on the route will be unknown.The value of this parameter is quite important because it determines how close the node is to achieve maximal trust. It would be best to assign a low value trust value in an environment with many malicious nodes. If a route contain known nodes, the trust value of these nodes is use to base the assignment of initial trust value.

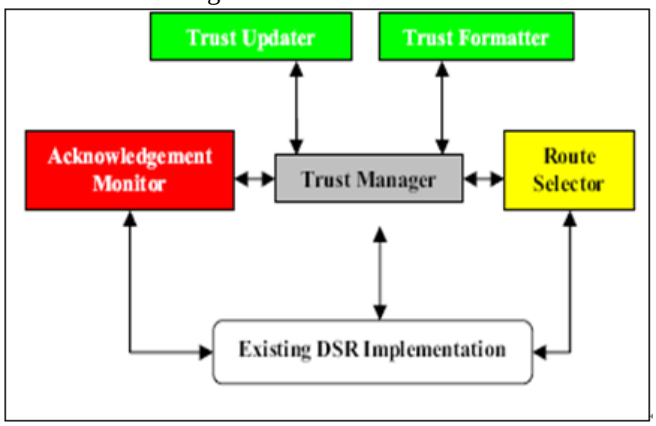

Figure4 Design diagram of modified DSR protocol

Initial Trust Value Estimation due to the importance of initial trust value, we need to determine optimal initial trust value to assign it to nodes when they are first time encountered.

Trust Updater Module Trust updater module is implements the function for updating trust. The trust value depends on a given node experience in a given situation. A function for updating trust value depends upon some parameters.

1 Previous trust value

2 Number of positive and negative experiences in past

3 The experience value.

Route Selector Module The route selector module is responsible to evaluate routes based upon trust value of the nodes in this route,and select a route on base of this evaluation.The routes are evaluated and the route with highest rating is then selected. that means the best route is considered which have the highest trust rating which means that has lowest number of malicious nodes.we can conclude that a node which has malicious node is not good because its always results in packet dropping.

There are two scenarios for route selection.when the route ratings are calculated, all routing scenarios must not take the destination of the packet in account, because the destination might be identifies as malicious node and therefore it has a low trust value.

This is necessary because the traffic is generated randomly for the simulations, and therefore malicious node may be also destination of the packets. All routing scenarios return maximum rating if route have only two nodes. Because it mean that destination is neighbor. If maximum rating is returned, the route is used without examining further routes. This is actually performance improvement compare to existing DSR protocol. Where all routes to a destination are examined even though the destination is neighbor node.

Route Selection Scenario 1 The first scenario will return the average trust value of all nodes in a route. Actually, this

IACSIT International Association of Computer Science and Information Technology WWW.IACSIT.ORG

scenario presents the issue that route containing nodes with very low trust values might still be rated high as illustrated in table 1.

Route Selection Scenario 2 The second scenario evaluates the nodes based on the average value of past experiences. Only 5 past experiences are remembered for this scenario to calculate the average value of experiences. I n this scenario nodes with a high trust value that suddenly start to drop packages will be identified faster than by using trust value.

In table 2 initial values for a node was (0.5). After three positive and two negative experience value, the average of the experiences is (0.2) where the trust value of node is (0.32). However, routing scenario 2 require more computations compared to scenario.1 because it uses experiences not only the trust values.

TABLEI. ROUTE SELECTION SCENARIO 1

Route	**Trust Values**				
	Node 1	***Node2***	***Node3***	***Node4***	
1	0.3	0.8	0.5	0.2	0.45
2	1	1	-1	1	0.75

*Trust Manager Module*The Trust manager module stores trust information about all known nodes during run time, and it offers method to query for information about stored trust values.

VIII. SIMULATION AND RESULTS

To evaluate the effectiveness of the proposed scheme, we simulated the scheme in NS-2.

A. Simulation Set-up

The simulation parameters are listed in Table 3. We implement the random way point movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s and the maximum simulation speed. All benign nodes execute the trust model for the duration of the simulation. The TUI value is set to 5 seconds, which has been found optimal in prior experiments for networks where the nodes have a maximum speed of up to 20 m/s with a transmission range of 250 meters.

The performance metrics are obtained through ensemble averaging by simulations, network with a different mobility and connection pattern.

TABLEII. ROUTE SELECTION SCENARIO 2

Experiance #	**Experiance Value**	**Trust Value**	**Avg Of This Experiances**
1	1	0.55	1
2	1	0.60	1
3	1	0.64	1
4	-1	0.47	0.5
5	-1	0.32	0.2

TABLEIII. SIMULATION PARAMETERS

Examined Protocol	DSR
Simulation time	900 seconds
Simulation area	1000 x 1000 m
Number of nodes	25
Transmission range	250 m
Movement model	Random way point
Propagation Model	Two-ray Ground Reflection
Maximum speed	20 m/s
Pause time	10 seconds
Traffic type	CBR (UDP)
Maximum Connections	10
Payload size	512 bytes
Packet rate	4 pkt/sec
Malicious nodes	2
Number of wormholes	1

B. Metrics

Performance of the proposed scheme is evaluated based on the metrics such as Throughput, Packet Loss By malicious node.

C. Simulation Outcomes

By using Trust Based Model Packet Dropping is reduced by 15% without using any cryptography mechanism. Throughput is increased up to 7-8% When trust based model is used in adhoc networks at the place of standard DSR Higher throughput is achieved using the trust based

DSR protocol.This is due to the fact that the trust level of any node not capable of sustaining the required traffic flow is automatically downgraded when it dumps the packets and some other node having a higher trust level is selected for the routing process. This feature helps to reduce traffic congestion onto trustworthy nodes by transferring the traffic load onto other available nodes in the neighbourhood ensuring a best-effort delivery for the generated traffic.

In case of detection of a wormhole by an intermediate node, all data packets leading towards the tunnel are dropped and a corresponding ROUTE ERROR packet is generated. The generation of these packets augments with the speed of the network as the colluding nodes are constantly varying their positions in the network.

This primarily leads to an increase in the packet overhead when the trust based DSR protocol is used. The probability of detection of wormholes significantly increases with speed.

At higher speeds the number of interactions with the nodes creating the wormhole increase considerably. This helps to spread trust information in the network at a appreciably higher rate. Up to 60% of the nodes executing the trust based DSR protocol were able to correctly identify at least one end of the wormhole. However, with increased mobility, the probability of detection of at least one colluding node by all network nodes becomes almost 100%.

Similarly, the detection probability for benevolent behaviour also follows a similar trend under increasing speeds.

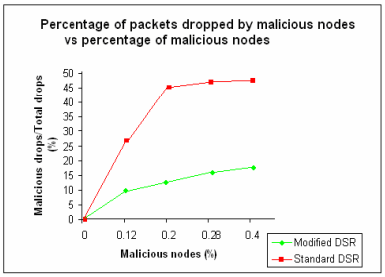

Figure5 packet dropped by malicious nodes vs percentage of malicious nodes

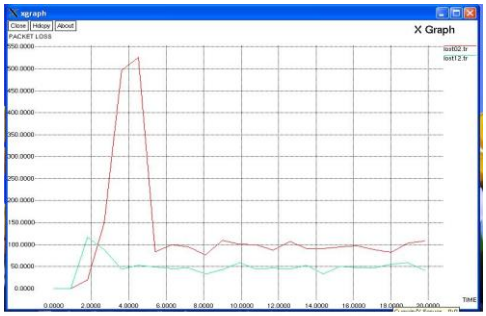

Figure6 X-GRAPH Packet loss VS Time

A number of nodes, whose behaviour pattern could not be analysed, were primarily those who were not part of any data connection during the simulation. The standard DSR protocol, does not take into account the trust levels of the nodes and so we see that a number of packets were tunnelled through the wormhole.

In contrast, each node using the trust based routing scheme takes into account the behaviour of the next node before forwarding a packet and so the total number of tunnelled packets drops appreciably. It can also be observed that at varying speeds, there are still some packets which are routed through the wormhole. The justification for such an occurrence is that the wormhole detection mechanism is based upon a minimal threshold (presently set to consecutive modification of two DSR source route headers) before it stops the data communication through the wormhole. This permits a small number of data packets to permeate the wormhole.

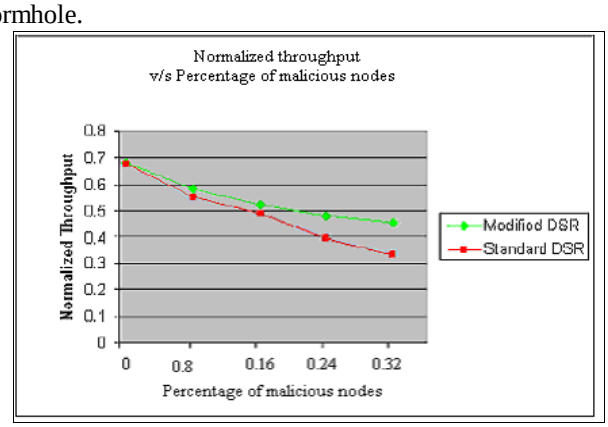

Figure7 Throughput versus percentage of malicious nodes

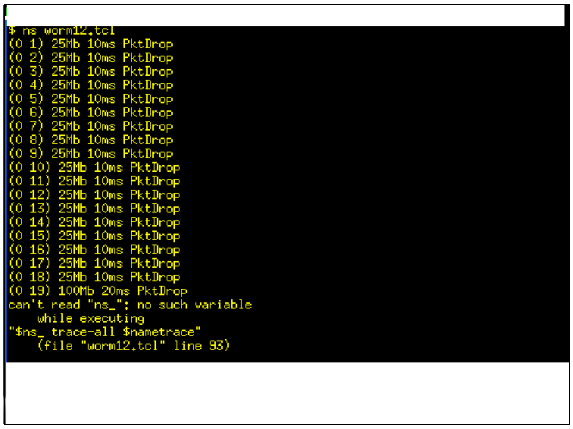

Figure8 All Packet Dropped By Maliciuous node-0

IX. Conclusion

A wormhole is one of prominent attack that is formed by malicious colluding nodes. The detection and evasion of such wormholes in an ad-hoc network is still considered a challenging task. In order to protect from wormholes, current security-based solutions propose the establishment of ad-hoc networks in a controlled manner, often requiring specialised node hardware to facilitate deployment of cryptographic mechanisms. In this paper, we have deviated from the customary approach of using cryptography and instead employ a trust-based scheme to detect and evade wormholes. In our scheme, we derive trust levels in neighbouring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes. Through extensive testing, we have established that the trust model can effectively locate dependable routes through the network in the presence of a wormhole in the network. The routes established in this manner may not be the shortest in terms of number of hops,but they definitely contain nodes which have been found more trustworthy than the others. By using Trust Based Model Packet Dropping is reduced by 15% without using any cryptography mechanism and throughput is increased up to 7-8%.

Future work related to this topic will focus on additional security enhancements for routing protocols of mobile ad hoc networks.

References

[1] Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks,” in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976-1986,2003.

[2] S. Capkun, L. Buttyan, and J. Hubaux, “SECTOR: Secure tracking of node encounters in multihop wireless networks,” in Proceedings of the ACM Workshop on Security of AdHoc and Sensor Networks, pp. 2132, 2003.

[3] E. W. Dijkstra, “A note on two problems in connection with graphs,” Numerische Mathematik, vol. 1,pp. 269-271, 1959.

[4] C. Hu, A. Perrig, and D. B. Johnson, “Ariadne:A secure on-demand routing protocol for ad hoc networks,” in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 12-23, 2002.

IACSIT International Association of Computer Science and Information Technology WWW.IACSIT.ORG

[5] C. Hu and D. B. Johnson, "Caching strategies in on-demand routing protocols for wireless ad hoc networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 231-242, 2000
[6] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium.
[7] A. Josang, "The right type of trust for distributed systems," in Proceedings of the ACM New Security Paradigms Workshop, pp. 119–131, 1996.
[8] D. B. Johnson, D. A. Maltz, and Y. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," IETF MANET, Internet Draft (workin progress), 2003.
[9] NS, The Network Simulator, http://www.isi.edu/nsnam/ns/, 1989.
[10] A. Perrig, Y. C. Hu, and D. B. Johnson, Wormhole Protection in Wireless Ad Hoc Networks, Technical Report TR01-384, Department of Computer Science, Rice University, 2001.
[11] M. Royer and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications Magazine, vol. 6, no. 2, pp. 46–55, 1999.
[12] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe), pp. 51–60,2004.
[13] H. Yuen and R. D. Yates, "Inter-relationships of performance metrics and system parameters in mobile ad hoc networks," in Proceedings of the IEEE MILCOM, vol. 1, pp. 519–524, 2002.
[14] A. A. Pirzada and C. McDonald, "Kerberos assisted authentication in mobile ad-hoc networks, in Proceedings of the 27th Australasian Computer Science Conference (ACSC), 2004.
[15] Master Thesis Group Key Agreement for Ad Hoc Networks by Lijun Liao Date: 06 July 2005 Supervisor: M.Sc. Mark Manulis.
[16] A Thesis in TCC 402 Presented to The Faculty of the School of Engineering and Applied Science University of Virginia by Jackson Kwok March 23, 2004.
[17] TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos University of California, Riverside.
[18] Y. C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM, 2003.
[19] S. Capkun, L. Buttyn, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 2003.
[20] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in ACM Workshop on Wireless Security (WiSe 2003), September 2003.
[21] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy,"Dawsen: a defense mechanism against wormhole attacks in wireless sensor networks", IN Second International Conference on Innovations in Information Technology (IIT'05).