Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE ROUTING IN MANET USING ASYMMETRIC GRAPHS

[1]GUNDALA SWATHI, [2]Y.HARSHAVARDHAN ,[3] R.SARAVANAN

Department of School of Information technology and Engineering,
VIT University, Vellore.
E mail: gundalaswathi@vit.ac.in

ABSTRACT

Identification of neighbours plays a major role of many protocols for wireless Adhoc networks and also the process of network paths in a network plays an important role. Wormhole attack is a major issue in networks. This type of attack causes the opponent to collects packets from one location and channels them to other location and retransmits them into the network. To avoid the problem of wormhole attack, so far we have several mechanisms like packet leashes for detecting against wormhole attack, a counter measure using directional antennas. Mobile Secure Neighbour Discovery Protocol performs a measure of security against wormhole attack by participating mobile nodes. In this paper we uses graph rigidity, Laman theorem for wormhole avoidance and forbidden graph for wormhole detection. By using these graphs we will provide a better solution to overcome the problem of wormhole attack in wireless Adhoc networks.

KEYWORDS: *Security, Mobile Adhoc Networks Identification Of Neighbours, Forbidden Graph, Rigid Graph, Multidimensional Scaling.*

1. INTRODUCTION

Identification of neighbours [1] defines determining whether a node is directly communicating according to the designed procedures of network or not. It can also be defined as the nodes which lie in the highest communication range of a particular node in a mobile Adhoc network. Freshly, there are so many identity measures have been planned for Identification of Radio Frequency systems. Due to the propagation delay in networks, if we implement these systems by using these procedures, the wastage of time is more. So, mostly the current identification of neighbour protocols are working under the control of slotted ALOHA system.

We use this, where the nodes which are identified [2] are instantaneously updated after the react frame. In this model, the time is slotted and all the packets are of same length. Here one full slot is packet transmission time. If the packets are transmitted in next slot, it is possible only after the packets arrive. The data rate which is low is used by slotted ALOHA. Military forces, setup a call to mobile telephony and in the contactless Radio Frequency Identification Technologies (RFID) are used in satellite communication networks At a time if more than one station transmits packets in the same slot, occurs collision, and the receiver can't receive the packets correctly. The transmission that happens only when there is exactly one packet transmitted in a slot called successful transmission. Otherwise the slot is called idle. Identification of neighbours is important issue in mobile Adhoc networks.

In wireless Adhoc networks direction-finding supports different types of secure routing protocols [3] to obtain Reliability, Availability, Confidentiality, Authenticity, Integrity, Non-repudiation services to protect the data from attackers. Routing supports so many attacks like Man-in-Middle attack, Denial of service attack, Black hole attack, wormhole attack... In our paper we will discuss about the wormhole attack. There are some requirements of routing protocols [9] are finding minimum route, Quick route reconfiguration when path is failed, Loop free

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

routing, Support Quality of Service, Security and privacy.

1.1 Security Services in Adhoc Wireless Networks:

To provide consistent data transfer in wireless networks and to save the system resources, a list of security services are mandatory. The different security services that are available in wireless Adhoc networks are as follows.

Availability: Availability is to be the belongings of a system or a system resource. These resources are available in working condition request by an authorised system entity. Outcomes of different types of attacks can cause the lessening in availability. Availability is a possession to be associated with various security services. Availability is one type of network service which protects a system for ensuring its availability. It concentrates on the security concern increased by denial-of-service attacks. It depends on power management, managing of system resources, access control service and other security services.

Confidentiality: Confidentiality is a security service which ensures the prevention of the information not to be disclosed to unauthorized users or unauthorized systems. Confidentiality is mainly used to restrict the accessibility of information. For example if you consider credit card transactions in the internet, the credit card number need to be transferred by customer to merchant and from merchant to transaction processing gateway network. In this case the confidentiality is provided by the card number is encrypted while transmitting so that the unauthorized user cannot access the card number. It can be accomplished by encrypting essential information using different types of encryption techniques. In a network it is used to protect data by entrusted parties.

Authenticity: Authentication is term which provides user to access a system which user wants to access. The identity of the user with security is provided by Authentication. Authentication ensures the identification of user individually by means of username and password. Every user has their own username and password, so that no unauthorized user cannot use the system to access the data.

Integrity: Integrity is a security service which prevents the modification of data by unauthorized users. It provides the approval only to the authorized users. To provide better integrity, the access to the data must be restricted and providing control of terminals and servers. In physical environment the data integrity can be achieved by following practices. (1) Servers need to be accessed only by the administrators. (2) Preventing transmission media not to be tapped.

Non-repudiation: It ensures that sending and targeting parties can never contradict or reject the sending or receiving the message. Non Repudiation is one of the security service in which it prevents the sender and receiver denying the message which is transmitted.

The secured routing protocols in wireless Adhoc networks include Authenticated routing for Adhoc network, Secure Efficient distance vector routing for mobile wireless Adhoc networks, Secure aware Adhoc routing, Co-operation of nodes fairness in dynamic Adhoc networks, Secure on demand routing protocol for Adhoc networks, Secure Adhoc on demand distance vector, Secure link state routing protocol.“Route Authentication” is also called “Neighbour router Authentication” [5]. It occurs only whenever receiving device modifications are exchanged between neighbour devices. It checks that whether a receiving device receives trustworthy routing information from a reliable source. It can be configured by using secure routing protocols in wireless Adhoc networks. Without neighbour Authentication, entrusted party could vulnerability the security of network traffic. Neighbour Authentication avoids any route changes from being received by the entrusted router. Authentication of neighbour works by the exchange of an Authenticating key which is already known to the sending and receiving nodes. Neighbour Authentication is of two types. They are Plain text Authentication and Message Digest Algorithm.

Protocols that use plain text Authentication are Disaster Recovery Plan server Agent(which describes how an organisation is to deal with potential disasters), (IS-IS) Intermediate System-Intermediate System (used to deal out the Internet Protocol information of all over a single independent System in an Internet Protocol network), Open Shortest Path First(link state routing protocol forms into a group of interior routing protocols by using a link state routing algorithm), Routing Information Protocol Version2 (which manages the router information within the self contained network like corporate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

local area network and the protocols that use the MD5[10] Authentication are Open Shortest Path Forwarding, Routing Information Protocol Version2, Border Gateway Protocol, Internet Protocol Enhanced Interior Gateway Routing Protocol(is also called a distance-vector interior gateway protocol used to call for each and every node to send all the data regarding of its routing table in a routing-update message at regular intervals to each of its neighbouring routers).MD5 sends a "message Digest" as an alternative of an authenticating key itself. It is formed using key and message.MD5 works similarly to plain text Authentication. For that, the router uses MD5 algorithm to produce "Message Digest" of key.

In this paper we will provide a better solution to the wormhole attack. It is a major issue in wireless mobile Adhoc networks. Wormhole attack enables an opponent with limited resources. To date, no general defences against wormhole attacks have been proposed. This paper will presents an analysis of wormhole attack and proposes a forbidden graph for wormhole detection and rigid graph for wormhole avoidance in wireless Adhoc networks. However a node mobility and rigidity graph concept are allow contribute nodes to identify the problems caused by wormholes.

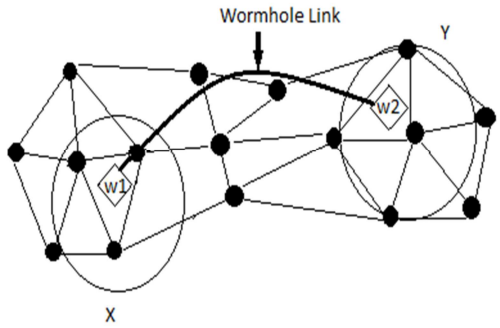


Fig.1. Exhibition Of A Wormhole Attack.W1 And W2 Represents The Wormhole Nodes Associated Through A Wormhole Link. As An Output Of The Attack, Nodes In Region X And Region Y Are Their Neighbours And Vice Versa.

The role of this article includes:

-Forbidden graph for finding out the presence of wormhole attack in wireless Adhoc network.

-By using the concept of rigid graph and Laman's theorem for avoiding the wormhole attack.

-Evaluating performance through suitable software and determine the wormhole detection.

2. RELATED WORK:

In order to televise information about complete network in a wireless Adhoc network, Identification of neighbours is very useful in initiation stage of network .Just this minute, Radio frequency Identification systems has a number of solutions that are suitable to global communication networks by using electromagnetic waves. So far if these solutions are developed in a network called long delay networks such as under water acoustic network [14], and then at most of the time will be wasted to delay. Underwater Acoustic Networking is an enable technology for applications in pollution monitoring and disaster prevention. To perform combined supervise tasks over a specified area, it comprises of number of sensors and vehicles that are deployed. To avoid that we made known two protocols methods for neighbour Authentication in slotted protocols. The first method can be accomplished by using Radio frequency identification systems. The second procedure is accomplished with the help of optimum number of probes. First method is hinge on the maximising the throughput in the procedure of an ALOHA. The second procedure not only reduces the detection time of the neighbours but also minimizes the power utilization. Currently the most identification of protocols is dependent on the system of slotted ALOHA. In this approach, latter the replied frame the acknowledgement frame will be transmitted immediately to the identified nodes. Hence they do not send their id after. Long delay networks such as underwater acoustic network are not directly used by the General identification procedures.

In wireless Adhoc networks, nodes that interact with directly using one hop with other node can be ascertained as neighbour nodes. There are several ways that are helpful in identifying the neighbours in a large network. We presuppose that the network is synchronized in the slotted case. In each and every probe the probing node send a time stamp of the communication time to the neighbours. By analyzing and distinctive this time value with the reception time, the replying nodes can calculate the transmission time to reach the probing node. After make a decision in which slots they are going to reply, the neighbours can begin transmitting their packets just before this calculated transmission time into the required slot.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A number of secure routing protocols have been projected for wireless Adhoc networks [11]. To restrict wormhole attack, a counter measure using directional antennas [13]. This method works by using a co-operative protocol where nodes share directional information to prevent wormhole end points from masquerading as entrusted neighbours. One more approach for detecting wormhole attack is for packet leashes [4]. Using directional antennas [7] to prevent wormhole attacks is for nodes to ascertain exact information about their neighbours. The directional neighbour discovery protocol doesn't perform on any co-operation between nodes and cannot prevent wormhole attacks. A temporal packet leashes puts a count on the duration of a packet that limit its travel distance.

Wireless Adhoc networks have self-configuration capabilities. Identification of protocols is fundamental requirements in building of self-organising networks [12]. Every node must know their neighbours in order to interact with them for any later communication. This can be obtained by using broadcasting methods [6] in networks. In wireless networks nodes are located centimetres to hundred meters away from each other, but they can communicate through their wireless transceivers. Broadcast communication is achieving recognition for capable and large scale data diffusion. Some of the broadcast distribution networks are the satellite broadcasting, wireless radio broadcast and IP multicast. In wireless Adhoc networks, the most significant challenge of the securing broadcast communication is source authentication. This predicament is convoluted by jointly counterfeit receivers and unreliable communication location where the sender doesn't resend lost packets.

Multidimensional scaling is a swap approach to factor analysis. Traditionally, swap approach can be described as the exchange of one security for another to change the maturity, quality of issue. In all approaches, the main goal obtained by these analyses is to detect a significant fundamental dimension which allows the user to clarify the observed similarities as well as dissimilarities of the objects which are investigated. In factor analysis, the similarity between different objects is articulated in the correlation matrix. A correlation matrix is one type of matrix which is defined as correlations between all pairs of data sets in a matrix. That is, i and j are row and column of the correlation matrix that is there is a correlation between i and j columns of the original matrix. Elements which are diagonal in the matrix will be 1.

Multidimensional scaling is used for analysing any kind of similarities as well as dissimilarity in the matrix, in addition to correlation matrices. In Multidimensional scaling the objects are compared in which each and every object has objective and perceived dimensions.

The goal of a Multidimensional scaling analysis is to find out the objects having spatial configuration which is known to compute the common resemblance. The spatial configuration must provide insight that how the subjects estimate the object in terms of small number of potentially not known dimensions. Collection is finished once the proximities derived, and by using the computer programs the multidimensional scaling solution must be solved. Almost all the Multidimensional scaling programs make a difference between traditional as well as non metric MDS.

Conventional Multidimensional scaling believes that the data, the proximity matrix. Proximity matrices form the data for multidimensional scaling. Asymmetric matrices are occurred to for providing displaying of the properties which are metric, for example measuring the distances in a map. Hence, like the distances in a traditional Multidimensional scaling space the intervals as well as ratios are used for the proximities as high as possible. A Data Matrix code is defines as it is a matrix barcode matrix which is a two-dimensional matrix which consists of both black as well as white "cells" in which modules are arranged in a rectangle or square pattern. The information is encoded either in numeric formatted data or text formatted data in which a strong metric assumption is considered behalf if the ratings related to human dissimilarities. While considering the meaningful order of proximities no metric multidimensional scaling is assumed. Distances order in a non metric Multidimensional scaling configuration reflects the proximities very good while information related to ratio as well as interval is of no significance. To understand the Multidimensional scaling outcome enhanced, the basic mechanisms, like classical Multidimensional scaling and no metric Multidimensional scaling in two multidimensional scaling, might be very helpful.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. TRADITIONAL MDS:

Multidimensional scaling is a conventional approach to the find the problems of basic dimensions, that manipulate how objects are evaluated by subjects. For this a mathematical result founded by knowing Euclidean distance between two cities p and q and x & y coordinates is defined by below formulae

$$d_{pq} = \sqrt{(x_p - x_q)^2 + (y_p - y_q)^2}$$

A problem named inverse problem is considered, in which by having distances by using this is it feasible to obtain the map Conventional Multidimensional scaling, it was first introduced by Toreros' in the year 1952, which addresses the above stated problem. It assumes that distances are considered as Euclidean. The first choice for multidimensional scaling space is Euclidean distances. The sum of non- 9 Euclidean distance measures, are partially reduced to some detailed research questions (cf. Borg & Groaned, 1997). Multidimensional scaling applications consist of [18] the data which measured are not distances in every map, but quite equal to proximity data. While applying classical Multidimensional scaling the proximities act like valid measured distances. For example data derived from the correlation matrix, but infrequently for direct distinction ratings. By using the traditional Multidimensional scaling the advantage is it specifies a systematic result, which requires no iterative measures.

3.1 Traditional MDS Algorithm:

Traditional Multidimensional scaling algorithms typically involve some linear algebra. The classical Multidimensional scaling algorithm rests on the fact that the coordinate matrix **X** can be derived by Eigen value [21] decomposing from scalar product matrix **B = XX′.** The problem of create **B** the closeness matrix **P** is solved by reproduce the squared proximities with the matrix **J = I−n^{-1} 11′.** This practice is called double centring.

4. RIGID GRAPH:

Rigidity is the structure property which does not bend or flex under an applied force. The antonym of rigidity is flexibility. In structural rigidity theory, structures are formed by collections of objects that are themselves rigid bodies, often supposed to take simple geometric forms such as straight rods, with pairs of objects connected by flexible hinges. A structure is rigid if it does not flex. That is, if there is no continuous motion of the structure that preserves the shape of its rigid components and the pattern of their connections at the hinges.

There are two essentially different kinds of rigidity. Finite or macroscopic rigidity means that the structure will not flex, fold, or bend by a positive amount. Infinitesimal rigidity means that the structure will not flex by even an amount that is too small to be detected even in theory. (Technically, that means certain differential equations have no nonzero solutions.) The importance of finite rigidity [19] is apparent, but infinitesimal rigidity is also crucial because infinitesimal flexibility in theory corresponds to real-world microscopic flexing, and consequent deterioration of the structure.

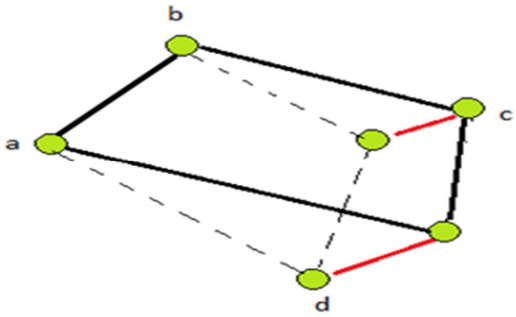


Fig.2. Rigid Graph With Flexibility

A rigid graph is an instil of a graph in a Euclidean space which supports a rigid structure. This type of structure created by substituting the edges by rigid rods and the vertices are elastic. The mathematical model of this structure is also called as the tensegrity structure. A graph which has at least 2n-3 edges is basic for a graph to be rigid.

A graph G = (V, E) consist of a set V of vertices and a set of E edges, with $|V| = n$, $|E| = m$ .The transfer of vertices V to points in R^d is to define a configuration p(V).In a graph , if the coordinates are algebraically independent over the rational it is said to a generic configuration. A structure G (P) [8] refers to a graph G along with a configuration. Generally a graph can have different frameworks with varying edge lengths. If there is a continuous twist from the given configuration to other, so that edge lengths are preserved, it is called elastic structure. If no such twist exists, it is called rigid.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. PRELIMINARIES AND PROBLEM FORMULATION:

Wormhole pretence [17] is a restrained and a dangerous hazard, because they can have an effect on communication by participating indirectly as network things. Moreover wormholes introduce noticeable modifications in a network. In this paper we concentrate more on dynamic nodes rather than static nodes in network. This division describes the models of the system and problem formulation.

6. SYSTEM MODEL:

Our system model is stimulated by mobile Adhoc networks. Mobile Adhoc networks are sovereign collection of mobile users that communicate over wireless links. In Adhoc network routing protocols attacks may disrupts network performance and reliability with their solution. Adhoc is one type of method for wireless devices to communicate and co-ordinate with each other. In a network, without involving central access, if the nodes/devices are communicate with each other then these nodes are said to be within the range of network. But in this type of attack nodes are in different ranges, each node has to use neighbouring nodes to reach other node, and then they are using in-between nodes to reach the node. In general routing, these devices use two methods to find out the routing. First one is source routing and other one is target routing. In source routing, it identify the whole routing, the transitional nodes to forward the message and the target routing specifies in header of message .Unit disk graphs [22] can be used to represent the nodes in the nodes in the form of a graph.

Mobile Adhoc network's has several salient characteristics [16] like self organising network, dynamic topology, Infrastructure less systems. Adhoc networking is attainment importance with enhance in number of well-known applications like military, disaster relief and health care. In wireless Adhoc networks, each and every node is capable of having on its own radio transceiver in addition to the clock having a range of capacity to support ranging operations. These nodes use bidirectional symmetric radio transmission for communication with a range RF. RG is the Ranging radius corresponds to the symmetric and the bidirectional.

A group of nodes can perform a set of limited operations of cryptography by using a pair of symmetric keys k [27]. In support of key establishment in Adhoc networks [26] we make use of any one of existing techniques. Accordingly, each pair of nodes source and destination shares symmetric keyK_{SD} [28]. The operations of cryptography includes authentication of message, encryption and hash calculations. Nodes can produce Nonce's which are in random order as they needed.

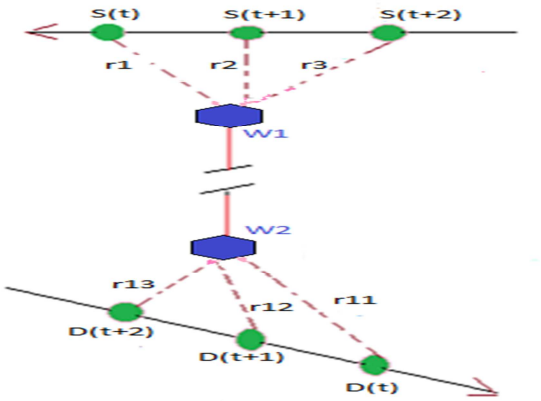


Fig.3. Two Mobile Nodes Communicate Through A Wormhole

Laman's states that for a graph G= (V, E) to be basically rigid [20] in the plane, it should have n vertices and 2n-3 self-regulating edges. Graphs that have more than 2n-3 edges, must be a subset F ⊆ E which suits two conditions: (1) $|F|$=2n-3 and (2) for all F'⊆ F, F' ≠ ϕ, $|F'| \leq$ 2k-3 , where k is the amount of vertices which are end points of edges in F'. In this paper, the number of edges E = r^2 where r is the number of ranges. After the third range, E > 2n-3 where n=2r. On the other hand in every sub graph F where r=3, then E=2k-3 and for every F' ⊆ F, $|F'| \leq$ 2k-3. So, by Laman's Theorem, the movement of each node is generically rigid. In a graph of rigidity, the range length can be calculated, if before ranges and travel distances are familiar. Since the distance travelled between range nodes and the lengths $r^2 - r$ edges are unknown to the wormhole. The left over length of r edges is also unknown .to the wormhole because the identity range cannot be acknowledged by a wormhole. Therefore, any non-produced graph will not be rigid if it is pretentious by the wormhole.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7. THREAT MODEL:

In this model, hazard has a group of fixed third parties shared across a geographical region [15]. Each and every attacker is capable like an exact node and has a comparable radio and range interfaces. Furthermore, each entrusted node has a subsequent network interface can able to converse using low latency links with other opponents.

The entrusted parties do not have facility to compromise a proper node. In mobile Adhoc networks the attacks are two types namely Internal and External attacks. These attacks are also called insider and outsider attacks. In this model attackers are external [23]. Nodes that are not belonging to the network carry the outside attacks. Actually, the attacks that occupied some portion of the network are called internal attacks. External attacks are less ruthless than the internal attacks. Since the internal attacks knows the secret information and contains access to confidential rights. The opponents do not have access to cryptographic keys. By using keys up to some extent we can avoid wormhole attack.

Opponents are organised into wormholes at the symbol level which performs fast relay attacks in that forward messages. The total delay of communications can be added negligible to the activities of wormhole. An attacker cannot be endlessly either collocated with or in the next of correct node otherwise the locality of mobile node and wormhole location would be impossible to distinguish between them.

8. PROBLEM FORMULATION:

Fig.2. provides a sketch out for understanding the attack of wormhole in wireless Adhoc networks. Node S moves through a region. When the nodes wants to communicate with each other they come into connect with one another. On the other hand, potential neighbours that are actually lying within the same neighbourhood have no assurance. Even though, data is protected by the encryption between the two communicating nodes that may really be linked through a wormhole. Nodes S and D are opponent neighbours, that may be convinced by the wormhole attack that they are. The usage of Asymmetric graph concepts is very helpful to check that whether the converse nodes are local to the same neighbourhood or not.

8.1 Forbidden Graph:

A forbidden graph characterization [24] is a method of indicating a family of graph or hyper graph, structures. In general, a structure *G* is a family member if and only if a forbidden substructure is not contained in *G*. The forbidden substructure might simply be a sub graph, or a substructure from which one might derive that which is forbidden. Thus, the forbidden structure might be one of the following three are Sub graphs, graph minors and homeomorphic sub graphs (also called topological mirrors).

8.2 Rigid Graph:

A rigid graph is a graph, which has a continual flow of sequential points of the formation sustaining bar conditions comes from a group of movements of all Euclidean space which are known as distance-retaining graphs. Generally non rigid graphs are flexible in nature. A graph *G* is commonly d-rigid if, for almost all configurations of P the structure G (p) is rigid inR^d. Graph rigidity is a key solution to this situation. Since the wormhole attack problem is not capable to know the distance passed through by each node it is not capable to manipulate ranging processes in a way that reasons a reliable group of ranges to be constructed. Laman's Theorem declare that graph *G*, arranged of rigid edges joined by elastic connections is nominally rigid in a plane if it has k vertices and 2k-3 self-regulating edges, and if every tempted sub graph on k vertices has at generally 2k-3 edges. A graph can be described as two nodes travelling with motion and equal range with its relative position. To support wormhole detection, in most of the cases the produced graph is rigid and rigidity possessions can be leveraged. A graph is rigid in this sense if and only if it has a Laman sub graph that spans all of its vertices. Thus, the Laman graphs are exactly the minimally rigid graphs, and they form the bases of the two-dimensional rigidity Matroids.

8.3 Ranging:

Ranging is a method which is used to determine the distance from one location to other location in a network. Ranging consists of three steps. The requirement of key is that each and every ranging node be required to pass through the length of the depict able path of the ranging phase. For this purpose, node travel in straight lines in anticipation of whichever enough ranges is composed or it is no longer possible to range.

Actually in synchronization step, it permits the participating nodes to calculate the approximately clock differences. When the last bit of the preamble is transmitted or received, the

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

transmitting or receiving nodes record the time. These timestamps will represent the sending/reception time. The next step, communication supplies a ranging signal. The last step, Data Exchange occupies a swapping of data that ends with both the nodes conscious of the range between them.

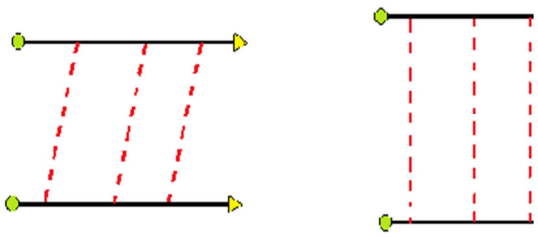


Fig.4. Travel Lines Are Equivalent And All Ranges Are Equal.

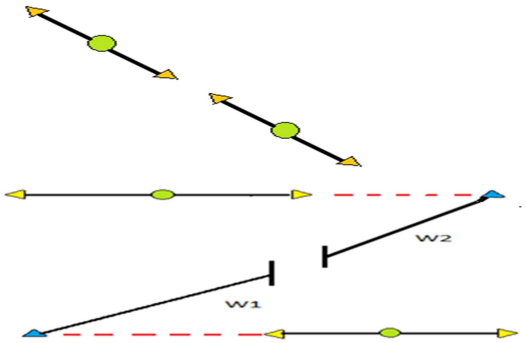


Fig.5. Due To Wormhole, All Points Are Collinear And It Seems That Collinear.

Degenerate cases

8.4 Synchronization:

In this step nodes S and D exchange two packets. Node S sends a request packet have nonce encrypted with a couple wise key SD and the hash of second nonce. If the packet is valid then using a message authentication code using pair wise key SD. Node D reply with a packet containing the decrypted nonce that is also authenticated. Both nodes accumulate the communication time and response time of two packets.

Synchronization

$S \xrightarrow{RF} D \quad \langle REQ, E_K SD\ \{N_D^r\}, H\{N^C\}, MAC_K SD\ \{.\}\rangle$

S t^S_{REQ} := Sending time of REQ

D t^D_{REQ} := Reception time of REQ

D If N_D^r is fresh and MAC is correct then:

$D \xrightarrow{RF} S \quad \langle REP,\ N_D^r,\ MAC_K SD\ \{.\}\rangle$

D t^D_{REP} := Sending time of REP

S t^S_{REP} := Reception time of REP

8.5 Communication:

Communication is the second phase; the node S is sent which ranges the preamble follow each and every single bit of nonce Ns at fixed intervals. Both D records, the coming time of the foreword and gathers the bits to rebuild the nonce.

Communication

$S \xrightarrow{RNG} * \quad \langle 1 \| N^C \rangle$

S t^S_{RNG} := Sending time of RNG

D t^D_{RNG}:= Reception time of RNG

D N^C_D:= Received RNG nonce

8.6 Data Swap:

During the Data switch over Step, node S encrypts the packet and sends it to node D via R_F which contains timing information as well as distance D_a travelled till the end operation of ranging. Nonce Ns is sent to compare the sets of timing data accurately. Node D stores this type of data since all the ranges are completed and calculated its range to S by using the ranging signal rate.

Data Exchange

S If D sends the exact REP, then

$S \xrightarrow{RF} D\ \langle ACK,\ E_K SD\ \{N^C,\ t^S_{REQ},\ ,t^S_{RNG},\ d_S\}\rangle$

D If MAC is correct and $N^C = N_D^C$ *and*

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\left|\left(t^{S}_{REP} - t^{S}_{REQ}\right) - \left(t^{D}_{REP} - t^{D}_{REQ}\right)\right| < \varepsilon$:

9. VERIFICATION:

Verification, which uses beginning checks, metric multidimensional scaling [29] and understanding the movement of nodes to find out the affect caused by a wormhole attack. The theory of verification is used to discover ranges and distances travel to examine if a result has been affected by a wormhole. If the two nodes are neighbours then the authentication confirms that it is a successful verification. Verification starts with beginning checks which includes ranges for a check that are so long, the range of neighbouring ranges whose varies by added than the collective distance travelled by the contribute nodes. Successful beginning checks are used by a loop which completes the testing of distance using multi dimensional scaling and a test of the fit of resulting co-ordinates. Here the output is evaluated and the greatest outcomes are used to making a decision about the presence or absence of wormhole.

In the verification, the first step is a set of beginning check that examines the distances for easily measurable fact of wormhole involvement.

The checks of beginning include

1.$r_i > R_{RNG} + \in$ Large ranges as $2 \times R_{RNG} + delay$, may be produced by wormhole.

2. $r_{i+1} = R_i \pm d_{Si} \pm d_{Di}$ When all the points are collinear, the change in length of the consecutive ranges is the direct results of adding and/or subtracting node travel distances.

3. $(r_i - d_{Si} - d_{Di}) < r_{i+1} < (r_i + d_{si} + d_{Di})$ The total length of the range r_i is not greater than the length of one node ranger_{i+1}. Each node travel between the ranges, it can be no smaller than their difference.

4. $(r_i = r_{i+1} = r_{i+2})$ & $(\sum_{i=1}^{r} d_{Si} = \sum_{i=1}^{r} d_{Di})$. All node ranges are equal the graph is not supported to a rigid.

Once the basic checks are complete the ranges r_i and travel distances d_{Si} and d_{Di} are transferred to Multi dimensional scaling in the form of a matrix D of size 2 NR (NR is the number of ranges collected).Between the two points in a graph we do not have a distance. For example, we do not have a range r_{12} between S (t) and D (t + 1) because mobile nodes are having mobility (hence, we have S (t) the same as S (t + 1)). Hence, the problem of Multi dimensional scaling is to solve only the partial ‘‘similarities’’ between the points. More purposely, matrix P is defined as follows:

$$P = \begin{matrix} 0 & S_{ij} & r_i & NaN \\ S_{ij} & 0 & NaN & r_i \\ r_{i-p} & NaN & 0 & D_{i-p.j-p} \\ NaN & r_{i-p} & D_{i-p,j-p} & 0 \end{matrix}$$

$S_{ij} = \sum_{k=i}^{j} d_{SK}$, $D_{ij} = \sum_{k=i}^{j} d_{DK}$, Nan indicates the absence of a distance between the points. We use p instead of NR, for condensed notation. The following steps summarize the algorithm of classical MDS:

1. Set up the matrix of squared proximities$\boldsymbol{P^{(2)}} = [P^2]$.
2. Apply the double centring: $\mathbf{B = -1/2J}\boldsymbol{p}^{(2)}\mathbf{J}$ using the matrix $\mathbf{J = I - }\boldsymbol{n}^{-1}\mathbf{11'}$. Where n is the number of objects.
3. Extract the m largest positive Eigen values $\boldsymbol{\lambda_1, \lambda_2}$ ..... $\boldsymbol{\lambda_m}$ of B and the corresponding m Eigen vectors $\mathbf{e_1 \ldots e_m}$.
4. An m-dimensional spatial configuration of the n objects is derived from the coordinate matrix $\mathbf{X} = \boldsymbol{E_m}\,\boldsymbol{\Lambda_m^{1/2}}$ where $\boldsymbol{E_m}$ is the matrix of m Eigen vectors and m is the diagonal matrix of m Eigen values of B, respectively.

The computational complexity of a fast classical MDS implementation is $O(N^2)$, where the proximity information is present in a N × N matrix (N = 2 × NR in our case). The output of MDS is X, the set of coordinates that describes each node’s path of travel. The goodness of MDS output is characterised by a stress factor

$$\sigma = \sqrt{\sum_{ij}\left(d_{ij} - d^{*}_{ij}\right)^2} / \sqrt{\sum_{ij} {d_{ij}}^2}$$

Since mobile nodes have knowledge about their path of travel (y = f(x)), we highlight the travel path y = f(x) does not need to be linear. For estimating the goodness of fit we use the norm of residuals:$\tau = \sqrt{\sum_i (y_i - \hat{y}_i)^2}$.

Algorithm. 1 Detection of wormhole attack

Step 1: check the structure of a graph
Step 2: If the graph is forbidden
Step 3: then it contains wormhole attack
Step 4: If the graph is not a forbidden graph
Step 5: then the graph doesn’t contain wormhole attack
Step 6: the nodes are trusted neighbours.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

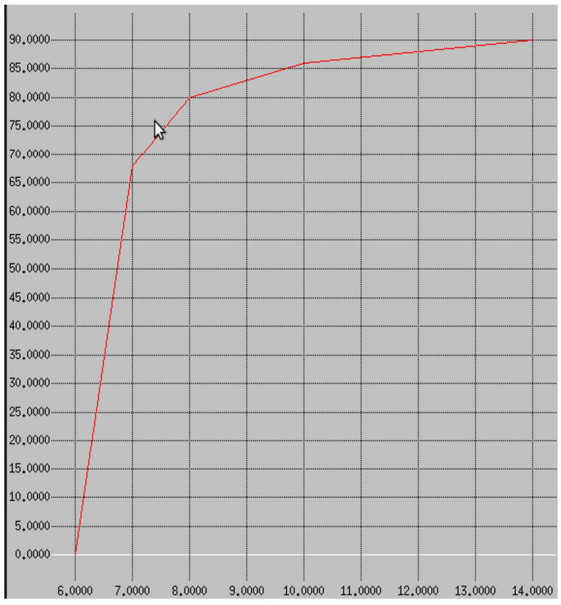
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm. 2 Avoidance of wormhole attack

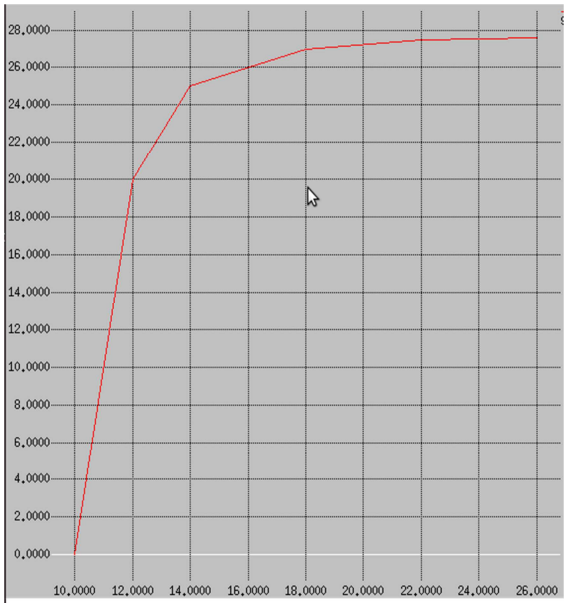
Step 1: check the graph structure
Step 2: If the graph supports k vertices and 2k-3 edges
Step 3: then that type of graph is called rigid
Step 4: the length of the ranges can be predicted if the rages and travelled distances are known
Step 5: wormhole is unable to know the distance travelled by each node
Step 6: By this method we can avoid the wormhole attack,

10. PERFORMANCE EVALUATION:

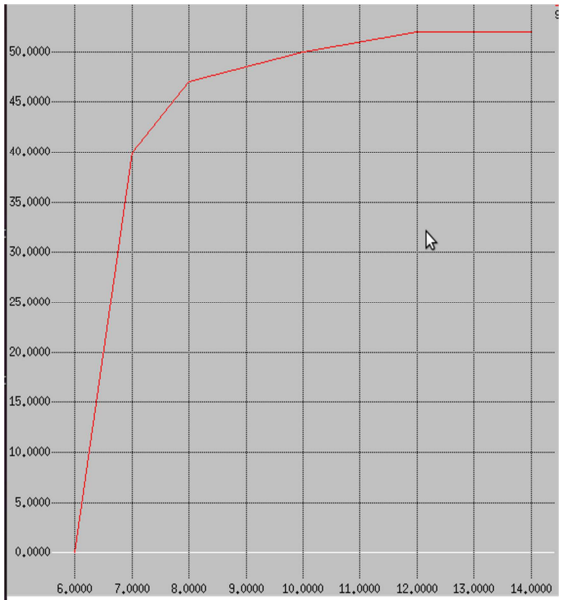
Our simulation testing is performed by using suitable software. Ranging and Movement were handled in a suitable software simulation of movement of a random waypoint model. Nodes move in certain area with the two ends occupied by a single wormhole. Both R_{RNG} and R_{RF} are set to some value. The speed of the node is chosen randomly at each waypoint of R_{RNG}. In Multidimensional scaling ranges detachment is in the form of matrix **D.**



(a)



(b)



(c)

Fig6. X-axis represents Time interval, Y-axis represents size of the packets.
In fig(a) represents General packet transmission, we are sending packets, in that it receives maximum number packets.
fig (b) represent Identification of wormhole, which receives a reduced amount of the packets.
fig (c) represents Avoidance of wormhole, which receives more number packets than fig (b)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

11. CONCLUSION AND FUTURE WORK:

Identification of neighbours plays a major role of various protocols for wireless mobile Adhoc networks. The capacity to determine secure suitable neighbours are key part of several network jobs. To the top of our understanding, in this paper we eradicate the wormhole attack by using forbidden graph and graph rigidity. Forbidden graph is used for detecting whether a wormhole attack is there in wireless Adhoc networks. Rigid graph which is used for avoidance of the wormhole attack in Adhoc networks. On progress and future work will include the concepts of localization errors, travel errors and ranging errors.

REFERENCES:

[1] Radu Stoleru, Haijie Wu, Harsha Chenji, Secure neighbor discovery and wormhole localization in mobile Adhoc networks, in:Proccedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems 2012.

[2] H. Chenji, R. Stoleru, H. Wu, Secure neighbour discovery in mobile Adhoc networks, in: Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems 2011.

[3] P. Papadimitratos, Z. Haas, Secure routing for mobile ad hoc networks, in: Proceedings of the Communication Networks and Distributed Systems, 2003.

[4] Y. Hu, A. Perrig, and D. Johnson, Packetleashes: a defence against wormhole attacks in wireless networks, in: Proceedings of the International Conference on Computer Communications, 2006.

[5] M. Poturalski, P. Papadimitratos, and J. Hubaux, Secure neighbour discovery in wireless networks: formal investigation of possibility, in: Proceedings of the ACM Symposium on network Information, 2009.

[6] B. Bellur and R. G. Ogier, "A reliable, efficient topology broadcast protocol for dynamic networks," in Proc. 18th Ann. Joint Conf. IEEE Comput. Commun. Soc., Mar. 1999, pp. 178–186.

[7] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proc. Symp. Netw. Distrib. Syst. Security, Feb. 2004.

[8] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," ACM Wireless Netw., to be published.

[9] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Proc. 7th Int. Workshop Security Protocols, Berlin, Germany, 1999.

[10] D. Touch, "Performance analysis of MD5," in Proc. ACM Conf. Appl., Technologies, Architectures, Protocols Compute. Communication, Aug. 1995, pp. 77–86.

[11] C. Karlof and D. Wagner. Secure Routing in Sensor Networks: Attacks and Countermeasures. First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.

[12] P. Papadimitratos, Z. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modelling and Simulation Conference, January 2002.

[13] C. Sanstivanez and J. Redi. On The Use of Directional Antennas for Sensor Networks. Military Communications Conference (MILCOM 2003), October 2003

[14] I.Akyildiz, D.Pompili and T. Melodia, "Underwater acoustic sensor networks: Research challenges," Ad Hoc Networks Journal, Elsevier, March 2005, vol. 3, Issue 3, pp. 257-279.

[15] S.Toumpis and A.Goldsmith, "Capacity regions for wireless ad hoc networks," IEEE Trans. Wireless Commun., vol.2, pp.736-748, July 2003.

[16] Vesa Karpijoki: Security in Adhoc Networks, 2001.

[17] R. Maheshwari, J. Gao, S. Das, Detecting wormhole attacks in wireless networks using connectivity information, in: Proceedings of the International Conference on Computer Communications (Infocom), 2007.

[18] R. Golledge, Multidimensional Scaling Review and Geographical Applications, Association of American Geographers, 1972.

[19] I. Streinu, L. Theran, Combinatorial genericity and minimal rigidity, in: Proceedings of the Symposium on Computational Geometry (SCG), 2008.

[20] B. Servatius, H. Servatius, Generic, abstract rigidity (private communication), 1999.

[21] U. Brandes, C. Pich, Eigen solver methods for progressive multidimensional scaling of large data, in: Proceedings of the International Conference on Graph Drawing (GD), 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[22] Breu, H., and Kirkpatrick, D. G. Unit disk graph recognition is np-hard. Compute. Geometric. Theory Appl. 9, 1-2 (1998).

[23] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, J.-P. Hubaux, Secure neighborhood discovery: a fundamental element for mobile ad hoc networking, IEEE Communications Magazine 46 (2) (2008) 132–139.

[24] Shinya Fujita, Michitaka Furuya, Kenta Ozeki , forbidden graph, Department of Mathematical Information science Toriba, Maebashi, Gunma, Japan, Tokyo University of Science, Kagurazaka, Shinjuku-ku, Tokyo Hitotsubashi, Chiyoda-ku, Tokyo, Japan.

[25] G. Laman On graphs and rigidity of plane skeletal structures Journal of Engineering Mathematics, 4 (4) (1970), pp. 331–340 [SD-008]

[26] Z. Li, J.J. Garcia-Luna-Aceves Non-interactive key establishment in mobile ad hoc networks,Ad Hoc Networks, 5 (7) (2007), pp. 1194–1203 [SD-008]

[27] S. Zhu, S. Xu, S. Setia, S. Jajodia, Establishing pair wise keys for secure communication in ad hoc networks: A probabilistic approach, in: Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP), 2003. [SD-008]

[28] H. Dahshan, J. Irvine, Authenticated symmetric key distribution for mobile ad hoc networks, in: Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2008. [SD-008]

[29] I. Borg, P. Groenen, Modern Multidimensional Scaling. Series in Statistics, Springer, 1997.

.