Reviewing MANET Network Security Threats

Priyanka Sharma[1], Dr. Surjeet Dalal[2]

[1]Student, M. Tech, ESEAR, Ambala
[2]Associate Professor, Dept. of CSE, E-Max group of Institutions, Ambala

***Abstract*— In the last decade, mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network. In this paper, we present a survey of the main types of attack at the network layer, and we then review Sybil attack. We show through simulation that Sybil attack can be prevented by proposed solution Finally, we identify areas where further research could focus.**

***Keywords*— MANET, Network Security, Attacks.**

I. Introduction

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly – dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network [1][2]. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table). MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

II. ATTACKS IN MANETS

Various types of network layer attacks or intrusions are known for MANETs. In this Section we first present a classification of major network layer attacks and introduce some individual attacks. We then illustrate some major network layer attacks.

Classification of Network Layer Attacks

Network layer attacks in MANETs can be divided into two main categories, namely passive attacks and active attacks, as shown in Figure 2.

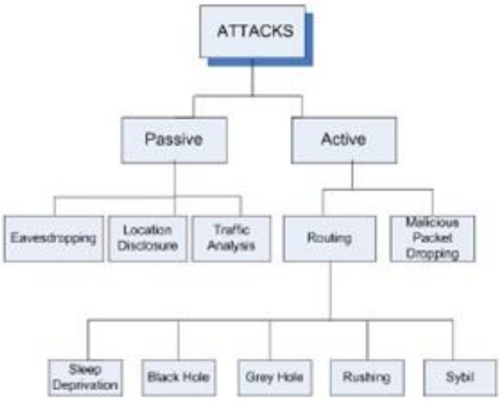

Fig1.

1) **Passive Attacks** : Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. This in turn can lead to the disclosure of critical information about the network or nodes such as the network topology, the location of nodes or the identity of important nodes. Some examples of passive attacks are as follows:

Eavesdropping

Because of the wireless links in MANETs, a message sent by a node can be heard by every device equipped with a transceiver and within radio range, and if no encryption is used then the attacker can get useful information. The sender and receiver usually have no means of knowing that this attack has taken place. Although in most cases eavesdropping is not considered to be a severe attack, it could provide vital information in some scenarios and therefore researchers have focused on minimizing it. For example in [92] the authors analyzed the risk of eavesdropping as a function of the transmission range of the nodes and their geographical distribution.

Traffic Analysis and Location Disclosure

Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the amount of data transmitted by nodes and the characteristics of the transmission. For example, in a battlefield scenario, a large amount of network traffic normally flows to and from the headquarters. Traffic pattern analysis therefore allows an intruder to discover the commanding nodes in the network. Even if the data in a message is protected by encryption, traffic analysis can still be performed to extract some useful information. Although passive attacks do not directly affect the network' functionality, in some MANET application scenarios, such as military communication, important information disclosure through traffic analysis
or simply eavesdropping could prove costly.

2) **Active Attacks** : In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks (as compared to passive attacks) disturb the operations of the network and can be so severe that they can bring down the entire network or degrade the network performance significantly, as in the case of denial of service attacks. Therefore, in this paper we have focused on active network layer attacks. Active attacks can be further divided into malicious packet dropping attacks and routing attacks, as shown in Figure 2.

Malicious Packet Dropping

A path between a source node and a destination node in a MANET is established using a route discovery process. Once this has been done, the source node starts sending the data packet to the next node along the path; this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. This process continues until the data packet reaches the destination node. To achieve the desired operation of a MANET, it is important that intermediate nodes forward data packets for any and all source nodes. However, a malicious node might decide to drop these packets instead of forwarding them; this is known as a data packet dropping attack, or data forwarding misbehaviour. In comparison to deliberately malicious behaviour, in some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves; alternatively the nodes may be selfish, for example saving their battery in order to process their own operations. Packet dropping attacks differ from black hole and grey hole attacks (see below) because there is no attempt to “capture” the routes in the network.

Routing Attacks

Both the reactive and proactive routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. Consequently, a malicious node can exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV [19] and DSR [20], allow intruders to launch a wide variety of attacks.

In the following we give examples of how different intrusive activities can cause various attacks in MANETs, illustrating them with AODV as the routing protocol.

Sleep Deprivation Attack

Sleep deprivation (SD) is a distributed denial of service attack in which an attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of the interaction is to keep the victim node out of its powerconserving sleep mode. In the authors consider an intruder that can cause SD of a node by exploiting the vulnerability of the route discovery process of the protocol through malicious route request (RREQ) flooding in the following ways:

Malicious RREQ Flooding 1: an intruder broadcasts a RREQ with a destination IP address that is within the network address range but where the corresponding node does not exist. This compels all the nodes to forward this RREQ because no one will have the route for this destination IP address.

Malicious RREQ Flooding 2: After broadcasting a RREQ an intruder does not wait for the ring traversal time, but it continues resending the RREQ for the same destination with higher TTL values. This is a significant denial of service attack when we consider the energy constrained operations of MANETs.

Black Hole Attack

Intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR, when a node requires a route towards the destination.

The node sends a RREQ and an intruder advertises itself as having the fresh route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The intruder, once chosen as an intermediate node, drops the packets instead of forwarding or processing them, causing a black hole (BH) in the network. The way the intruder initiates the black hole attack and captures the routes may vary in different routing protocols. For example, in AODV, the destination sequence number (dest_seq) is used to represent the freshness of the route. A higher value of dest_seq means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new dest_seq number larger than the current dest_seq number. In this way, the intruder becomes part of the route to that destination. The severity of the attack depends on the number of routes in the network the intruder successfully becomes part of.

Grey Hole Attack

A grey hole attack (GH) [24] is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. For example, the intruder may drop packets from specific source nodes, or it may drop packets probabilistically or drop packets in some other specific pattern. As we noted above, BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason.BH and GH attacks on the other hand comprise two tasks: the attacker first captures routes and then either drops all packets (BH attack) or some packets (GH attack).

Rushing Attack

In order to limit the control packet overhead, an on-demand protocol only requires nodes to forward the first RREQ that arrives for each route discovery. An attacker can exploit this property by spreading RREQ packets quickly throughout the network to suppress any later legitimate RREQ packets. For example, in AODV an intruder can forge and forward a rushed RREQ, assigning a higher source sequence (src_seq) number to it; the intruder will also transmit the packet earlier than specified in the AODV protocol (this is the sense in which it is a “rushing” attack). This causes any later legitimate RREQ to be suppressed, and increases the probability that routes that include the intruder will be discovered instead of other valid routes.

Sybil Attack

Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority to verify these identities. An attacker can exploit this property and send control packets, for example RREQ or RREP, using different identities; this is known as a sybil attack (SY) . This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other severe attack. In summary, we note that the motivation of intruders behind launching either packet dropping or routing attacks is to achieve a certain goal such as denial of service (i.e. making certain resources or services, such as applications, web access, printing, or routing, unavailable to the intended users). In addition, other goals of intruders might include partitioning the network, creating routing loops, discovering valuable information, or theft of resources.

III. MANET CHALLENGES

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include:

Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

Security and Reliability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobilityinduced packet losses, and data transmission errors.

Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

Multicast: Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

Location-aided Routing: Location-aided routing uses positioning information to define associated regions so that the routing is spatially oriented and limited. This is analogous to associatively-oriented and restricted broadcast in ABR.

IV. The Sybil Attack

It’s a digital dangerous world. Security and antivirus software is important for any network. One way security can break down is in a Sybil attack. Named after the case study of a woman with multiple personality disorder, a Sybil attack is a type of security threat when a node in a network claims multiple identities.

Most networks, like a peer-to-peer network, rely on assumptions of identity, where each computer represents one identity. A Sybil attack happens when an insecure computer is hijacked to claim multiple identities. Problems arise when a reputation system (such as a file-sharing reputation on a torrent network) is tricked into thinking that an attacking computer has a disproportionally large influence. Similarly, an attacker with many identities can use them to act maliciously, by either stealing information or disrupting communication. It is important to recognize a Sybil attack and note its danger in order to protect yourself from being a target.

First described by Microsoft researcher John Douceur, a Sybil attack relies on the fact that a network of computers cannot ensure that each unknown computing element is a distinct, physical computer. A number of authorities have attempted to establish the identity of computers on a network (or nodes) by using certification software such as VeriSign, employing IP addresses to identify nodes, requiring passwords and usernames, and so forth. However, impersonation, both in the real and digital worlds, is commonplace. Friends may share passwords, communities may share website registrations and some services provide a single IP address that is shared among users.

Sybil attacks have appeared in many scenarios, with wide implications for security, safety and trust. For example, an internet poll can be rigged using multiple IP addresses to submit a large number of votes. Some companies have also used Sybil attacks to gain better ratings on Google Page Rank. Reputation systems like eBay's have also been victims of this type of attack.

There are few sure-fire ways to protect a network from a Sybil attack, but there is a wide range of literature dedicated to discussing options for protection and verification of computing identities. One way is by using trusted certification in which a single, central authority establishes and verifies each identity via a certificate. Trusted certification is not foolproof, however, and it can use up large amounts of resources and bottleneck traffic on the network.

Another option is called resource testing. The aim of resource testing is to determine whether a collection of identities posses fewer resources than they would if they were independent. Resource testing scans computing power, storage space, network bandwidth and other parameters to determine if the collection is from a single, Sybil-attacking computer or a series of true identities.

Utilizing trusted devices is similar to using trusted certification to defend against a Sybil attack. In this case, identities are associated to specific hardware devices. Similar to a central authority creating certificates, there are few ways to prevent an attacker from attaining multiple devices.

It is important to know what threats are out there. In a typical home or office setting, a Sybil attack may not have as much direct effect as a virus or Trojan attack, but this type of attack can affect the fabric of internet commerce and communication. Understanding what a Sybil attack is and how to spot one is essential for any savvy internet user.

V. SYBIL ATTACKS IN AD HOC NETWORKS

An ad hoc network is composed of mobile, wireless devices, referred to as nodes, that communicate only over a shared broadcast channel. An advantage of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide Connectivity to nodes outside direct broadcast range.

Ad hoc routing protocols are used to find a path end-toend through the cooperative network [25, 14]. Each node needs a unique address to participate in the routing. Often addresses are assigned as an IP addresses or a unique media access channel (MAC) address. Because all communications are conducted over the broadcast channel, nothing but these identifiers are available to determine what nodes are present in the network.

In unsecured routing protocols, such as DSR or AODV, these address-based identifiers can be easily falsie by malicious nodes, which presents an opportunity for a Sybil attack.

However, allowing unauthenticated address presents a series of other attacks, including route direction, spoofing, and error fabrication [12]. Our methods work whether addresses are authenticated or not, though given the wide range of attacks possible against unauthenticated networks, Sybil attacks may not be the most significant problem present. Our methods will also work on disruption tolerant networks (e.g., [6]), however, just as such networks incur an extreme routing delay, there will be a corresponding large delay in successful sybil attack detection. Secured ad hoc networks can be classified into three broad groups, each of which can be susceptible to the Sybil attack.

PKI-based protocols. Much of the initial work in ad hoc network security focuses on secure routing [12, 28,13, 11, 24, 23]. A variety of protocols have been proposed to counter routing attacks, some of which require a central authority or other mechanism to distribute cryptographic material to nodes in the system prior to or during deployment. Systems involving a central authority are less flexible, and installing a central authority removes the chief advantage of ad hoc networks: the ability to form spontaneously from whatever nodes are available. Allowing nodes to join without pre-distributing keys leaves a potential Sybil attack.

Threshold-based protocols. To avoid the untenable requirement of a PKI, other protocols use threshold cryptography. In such scheme, a group of trusted nodes distributes cryptographic material only if a subset of that group agrees on the trustworthiness of new members [16, 32, 15]. Sybil attackers can additionally defeat schemes that rely on threshold cryptography because verifying the true number and independence of nodes in the network is difficult. If a Sybil attacker can generate identities to meet the threshold requirements it can effectively control the routing of the network.

Reputation Schemes. Other security mechanisms for ad hoc networks include protocols for determining and maintaining reputation information about nodes in the group [3, 18, 2, 21, 27]. Each node can develop trust in the other nodes that it believes are routing correctly. The Sybil attack undermines these protocols because a node can use multiple identities to falsely vouch for or otherwise support an identity that would otherwise gain a bad reputation. A reliance on cryptographic certificates or keys does not prevent the Sybil attack in general because one entity may be in possession of multiple keys. For example, if PKI credentials are simply purchased (e.g., through VeriSign), the PKI is reduced to a resource test of each identity’s wealth, which can be without bound. Unfortunately, implementing a stronger approach is problematic. This is because in practice it is untenable to create a foolproof system that can scale to a significant number of users to check identities for independence before the keys are issued. Deploying a foolproof systems touches on issues including physical security and attacks involving social engineering or physical force. It would require checking a person against some set of unforgivable documents; but even government-issued documents are forged regularly.

In existing technique they followed RSS (Received Signal Strength), so if any nodes with RSS greater than the given threshold will be considered as the attacker. This approach is totally not applicable for the MANET because mobile nodes may have various signal strength.

In order to prevent this attack a centralized approach is needed that will monitor the mobile nodes.

VI. PROPOSED SOLUTION

In the proposed approach, nodes connecting to MANET are monitored by server agent, the server agent manages the details of mobile node in a network like

- Behavior of the node
- Speed of the node
- Direction of the node
- Position of the node

This technique prevents the malicious node from attacking other nodes.

STEP 1.

The nodes participating in the networks to access service like internet registers its identity with the server agent, the server agent replies with unique ID to the requesting node.

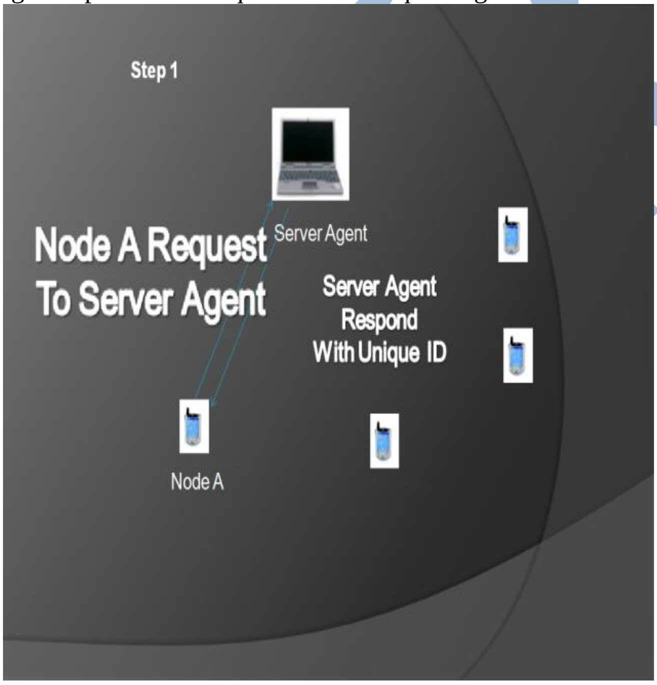
Step 1
Node A Request To Server Agent
Server Agent
Server Agent Respond With Unique ID
Node A

Fig 2.

STEP 2.

The source node sends route request with the current access point to the destination node .The current access point forwards the route request to the server agent.

STEP 3

The server agent verifies the source ID, then it accepts the route request from sender then it gathers the information of receiver using destination ID from the list.

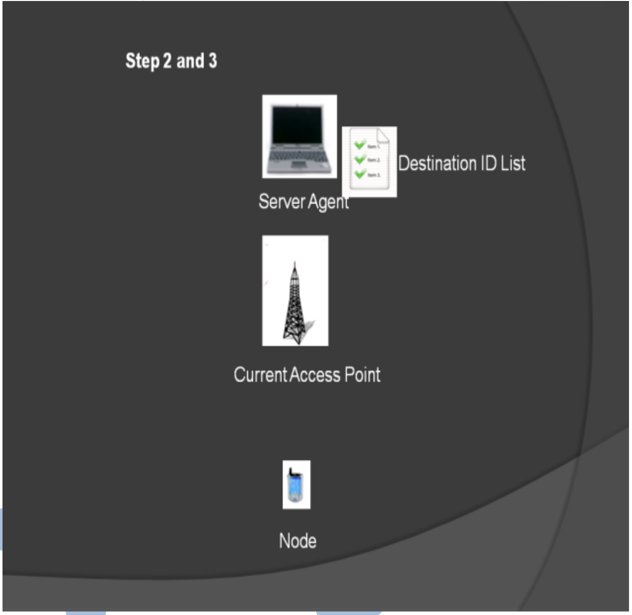

Fig 3.

STEP 4

The server agent then broadcasts the route request message using destination ID, the registered adjacent nodes that are nearer to the destination node which are ready to provide the service replies with the acknowledgement message to the server agent.

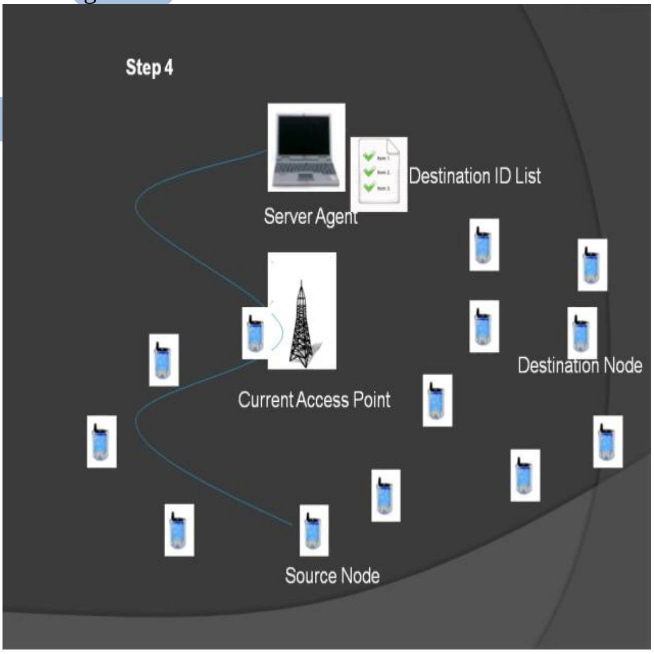

Fig 4.

STEP 5

The server agent chooses the adjacent node with the longest life time (the ability of the nodes to stay connected with the destination node) using the details collected from the ID, Such as nodes position, direction of motion and speed of the node.

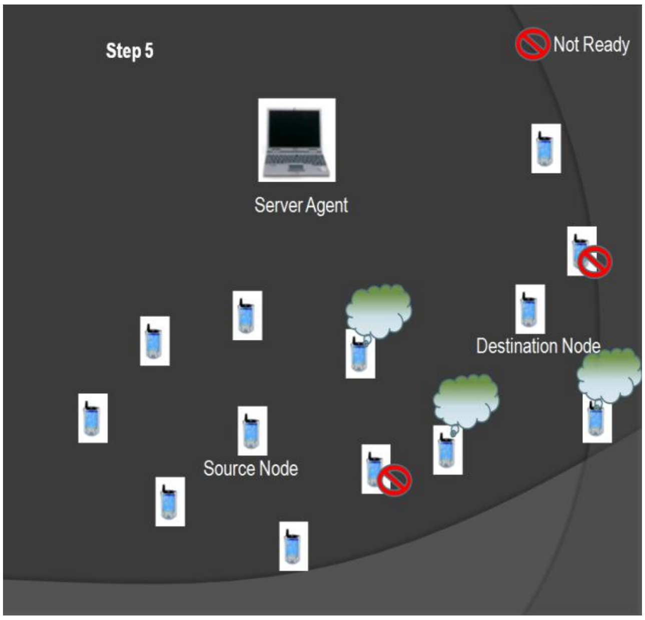

Fig 5.

STEP 6
Then the server agent provides route reply message for the source node, after this authentication process, source node starts sending data packets in a secure way.

STEP 7
In case any node moves away from the network, immediately the server agent replaces it with some other nodes to maintain the continuity of connection.

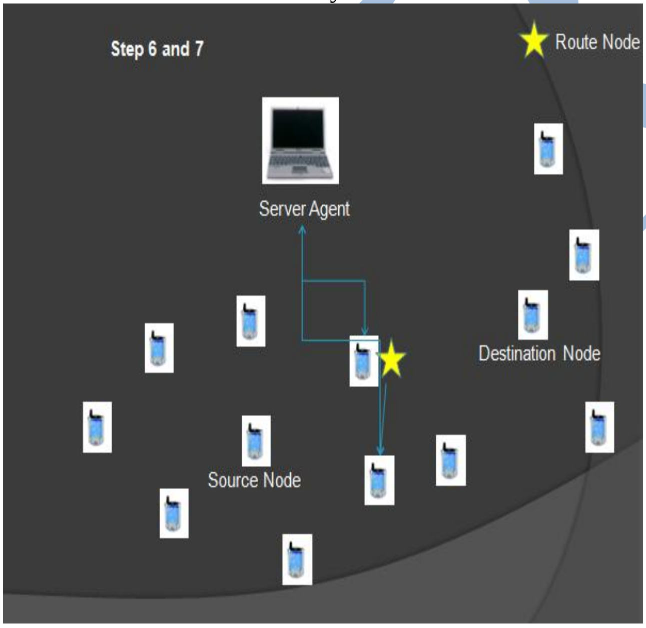

Fig 6.

References

[1]. O. Berthold, H. Federrath, and M. Kohntopp. Project anonymity and unobservability in the internet. In Computers Freedom and Privacy Conference 2000 (CFP), April 2000.

[2]. S. Buchegger and J. Le Boudec. Performance Analysis of the CONFIDANT Protocol. In Proc. Intl Symp on Mobile Ad hoc Networking and Computing, pages 226–236, June 2002.

[3]. S. Buchegger and J. Le Boudec. A Robust Reputation System for P2P and Mobile Ad hoc Networks. In Proc. Wkshp Economics of Peer-to-Peer Systems, June 2004.

[4]. N. Bulusu, D. Estrin, L. Girod, and J. Heidemann. Scalable Coordination for wireless sensor networks: Self-Configuring Localization Systems. In Proc. Intl Symp on Communication Theory and Applications, July 2001.

[5]. N. Bulusu, J. Heidemann, and D. Estrin. GPS-less Low Cost Outdoor Localization For Very Small Devices . IEEE Personal Communications, Special Issue on Smart Spaces and Environments, 7(5), October 2000.

[6]. J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine. Maxprop: Routing for vehicle-based disruption-tolerant networks. In Proc. IEEE INFOCOM, April 2006.

[7]. S. Capkun, M. Hamdi, and J. Hubaux. GPS-Free Positioning in Mobile Ad hoc Networks. In Proc. Hawaii Intl Conference on System Sciences, 2001.

[8]. S. Capkun, J. Hubaux, and L. Butty. Mobility helps security in ad hoc networks. In Proc. ACM Intl Symp on Mobile Ad hoc Networking and Computing, pages 46–56, June 2003.

[9]. A. Cheng and E. Friedman. Sybilproof Reputation Mechanisms . In ACM Wkshp on the Economics of Peer-to-Peer Systems, August 2005.

[10]. J. R. Douceur. The Sybil Attack. In Intl Wkshp on Peer-toPeer Systems, March 2002.

[11]. Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks. In Proc. Wkshp on Mobile Computing Systems and Applications, Jun. 2002.

[12]. Y. Hu and A. Perrig. A Survey of Secure Wireless Ad hoc Routing. IEEE Security & Privacy, 2(3):28–39, May/June 2004.

[13]. Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure OnDemand Routing Protocol for Ad hoc Networks. In Proc. Intl Conference on Mobile Computing and Networking, Sep. 2002.

[14]. D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. In Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[15]. A. Khalili, J. Katz, and W. A. Arbaugh. Toward Secure Key Distribution in Truly Ad hoc Networks. In Proc. Symp on Applications and the Internet Wkshps, January 2003.