SECURITY OPERATIONS OF VITAL ROUTING PROTOCOLS IN WIRELESS AD HOC NETWORKS

K.S.Saravanan,
Research Scholar,
Bharathiyar University,
Combatore,Tamilnadu,India.

Dr.N.Rajendran,
Principal,
Vivekanandha Arts and Science College for Women,
Sankari,Tamilnadu,India.

Abstract: In this Research paper we illustrate Security operations of Routing Protocols in Wireless Ad Hoc Networks. Routing operation are provides the communication protocol for data transfers between wireless devices. Conventional routing protocols aim does not deal with security, and are based on a mutual trust relationship between wireless devices. Wireless ad hoc network are week to security attacks due to their unique characteristics since it is a challenging task for routing protocols. We examined present the details of important secure routing protocols such as SRP, SAR, ARAN, ARIADNE, CONFIDANT and SEAD.

Keywords: Routing Protocols, Ad-hoc Networks, Security, attack

I.INTRODUCTION

Wireless networks provide rapid access to information and computing, eliminating the barriers of distance, time, and location for many applications ranging from collaborative, distributed mobile computing to disaster recovery, law enforcement and military communications. An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration [1]. Wireless Ad Hoc networks are not a pre-deployed infrastructure accessible for routing packets end-to-end in a network. In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper an effort has been made to evaluate various security designs proposed [2].

This article examines routing protocols designed for these ad hoc networks by first describing the operation of each of the protocols, the next section presents a discussion of four subdivisions of ad hoc routing protocols. Another section discusses current table-driven protocols, while a later section describes those protocols which are classified as on-demand. The article then presents many ad hoc wireless networks routing protocols are discussed; and finally, the last section concludes the article.

II.SECURITY ATTACKS

Classify routing attacks into five categories: attacks using impersonation, Modification, fabrication, replay, and denial of service (DoS).

a) Attacks using Impersonation

In impersonation attacks, an intruder assumes the identity and privileges of another node in order to consume its resources or to disturb normal network operation. An attacker node achieves impersonation by misrepresenting its identity. This can be done by changing its own IP or MAC address to that of some other legitimate node. Some strong authentication procedures can
be used to stop attacks by impersonation.

- **Man-in-the-Middle Attack :** In this attack, a malicious node reads and possibly modifies the messages between two parties. The attacker can impersonate the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked.

- **Sybil Attack :** In the Sybil attack, an attacker pretends to have multiple identities. A malicious node can behaves as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Sybil attacks are classified into three categories: direct/indirect communication, fabricated/stolen identity, and simultaneity. In the direct communication, Sybil nodes communicate directly with legitimate nodes, whereas in the indirect communication messages sent to Sybil nodes are routed through malicious nodes. An attacker can fabricate a new identity or it can simply steal it after destroying or temporarily disabling the impersonated node. All Sybil identities can participate simultaneously in the network or they may be cycled through [3].

b) Attacks Using Modification

This attack disrupts the routing function by having the attacker illegally modifying the content of the messages.

- **Misrouting Attack:** In the misrouting attack, a non-legitimate node sends data packet to the wrong destination. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.
- **Detour Attack:** In this type of attack, the attacker adds a number of virtual nodes in to a route during the route discovery phase. As a consequence, the traffic is diverted to other routes that appear to be shorter and might contain malicious nodes which could create other attacks. The attacking node can save energy in a detour attack because it does not have to forward packets to that destination itself. This attack is specific to source routing protocols.
- **Blackmail Attack:** This attack causes false identification of a good node as malicious node. In ad hoc wireless networks, nodes usually keep information of perceived malicious nodes in a blacklist. An attacker may blackmail a good node and tell other nodes in the network to add that node to their blacklists as well, thus avoiding the victim node in future routes.

c) Attacks using Fabrication

In fabrication attacks, an intruder generates false routing messages, such as routing updates and route error messages, in order to disturb network operation or to consume other node resources. A number of fabrication messages are presented next.

- **Resource Consumption Attack :** In this attack, a malicious node deliberately tries to consume the resources (e.g. battery power, bandwidth, etc.) of other nodes in the network. The attack can be in the form of unnecessary route requests, route discovery, control messages, or by sending stale information. For example, in routing table overflow attack, a malicious node advertises routes to non-existent nodes, thus causing routing table overflow. By using packet replication attack, an adversary consumes bandwidth and battery power of other nodes.
- **Routing Table Poisoning :** In this attack, a malicious node sends false routing updates, resulting in sub-optimal routing, network congestion, or network partition. Rushing Attack A malicious node in rushing attack attempts to tamper RouteRequest packets, modifying the node list, and hurrying its packet to the next node. Since in on demand routing protocol only one RouteRequest packet is forwarded, if the route requests forwarded by the attacker are first to reach target (destination), then any route found by the route discovery mechanism will include a path through the attacker.
- **Black Hole:** In this type of attack, a malicious node advertise itself as having the shortest path to all nodes in the network (e.g. the attacker claims that it is a level-one node). The attacker can cause DoS by dropping all the received packets. Alternately, the attacker can monitor and analyze the traffic to find activity patterns of each node. Sometimes the black hole becomes the first step of a man-in-the-middle attack.
- **Gray Hole :** Under this attack, an attacker drops all data packets but it lets control messages to route through it. This selective dropping makes gray hole attacks much more difficult to detect then blackhole attack.

d) Replay Attacks

In the replay attack, an attacker retransmits data to produce an unauthorized effect. Examples of replay attacks are wormhole attack and tunneling attack.

- **Wormhole Attack :** In the wormhole attack , two compromised nodes can communicate with each other by a private network connection. The attacker can create a vertex cut of nodes in the network by recording a packet at one location in network, tunneling the packet to another location, and replaying it there. The attacker does not require key material as it only needs two transceivers and one high quality out-of-band channel. The wormhole can drop packets or it can selectively forward packets to avoid detection. It is particularly dangerous against different network routing protocols in which the nodes consider themselves neighbor after hearing a packet transmission directly from some node[4].
- **Tunneling Attack:** In a tunneling attack, two or more nodes collaborate and exchange encapsulated messages along existing data routes. For example, if a RouteRequest packet is encapsulated and sent between two attackers, the packet will not contain the path traveled between the two attackers. This would falsely make the receiver conclude that the path containing the attackers is the shortest path available [5].

e) Denial of Service (DoS)

In the DoS attack, an attacker explicitly attempts to prevent legitimate users from using system services. This type of attack impacts the availability of the system. An ad hoc wireless network is vulnerable to DoS attacks because of its dynamic changing topology and distributed protocols. Examples of DoS attacks include:

- **Consumption of Scarce Resources:** Attacker can consume valuable network resources (e.g. bandwidth, memory and access points) so that the entire network becomes unavailable to users.
- **Destruction or Alteration of Configuration Information:** In this DoS attack, an attacker attempts to alter or destroy configuration information, thus preventing legitimate users from using the network. An improperly configured network may not perform well or may not operate at all [6].

III. SECURITY SERVICES AND CHALLENGES:

In order to guarantee a dependable information transport over the communication networks and to guard the system resources, a number of security services are mandatory. Based on their objectives, the protection services are confidential in five categories: availability, confidentiality, authentication, integrity and non repudiation [7].

(a) Availability: Availability implies that the requested services (e.g. bandwidth and connectivity) are obtainable in

a opportune approach while there is a possible problem in the system. Accessibility of a network can be temper for instance by reducing off packets by resource reduction attacks.

(b) Confidentiality: Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Confidentiality can be achieved by using different encryption techniques so that only the legitimate communicating nodes can analyze and understand the transmission. The content disclosure attack and location disclosure attack reveals the contents of the message being transmitted and physical information about a particular node respectively.

(c) Authenticity: Authenticity is a network examines to agree on a user's uniqueness. Without verification, an attacker can imitate any node, and in this way, one by one node, it can gain organize above the complete system.

(d) Integrity: Integrity guarantees that in order passed on flanked by nodes has not been tempered in the broadcast. Information can be altered both deliberately and unintentionally (for example through hardware glitches, or in case of ad hoc wireless connections through interference).

(e) Non-repudiation: Non-repudiation ensures that the information inventor cannot refute having sent the information. This service is practical for uncovering and separation of compromised nodes in the network. Many verification and secure routing algorithms implemented in ad hoc networks rely on trust-based concepts. The fact that a message can be credited to a exact node helps making these algorithms more protected.

IV.SECURITY OPERATIONS SOLUTIONS FOR ROUTING PROTOCOLS:

Secure Routing Protocol (SRP):

SRP is a further protocol addition that can be applied to many of the on demand routing protocols used today. SRP defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information. Secure Routing Protocol (SRP) based on Dynamic Source Routing (DSR). There is a security association (SA) between the source node S and the destination node D without the need of cryptographic validation of the communication data by the intermediate nodes. By using the SA, the principles that participated in the exchange can verify each other. The source and destination share a secret key KS, T, which is negotiated by the SA. An attack is mounted in this protocol by only two colluding nodes during a single route discovery. MAC (Message Authentication Codes) plays an important role in SRP. The source node S sets up the route discovery and constructs a route request packet by a pair of identifiers: a query sequence number and a random query identifier. The source and destination and the unique query identifiers are the input for the calculation of the MAC, along with a shared key KS, T. When receiving a route request, if it is a fresh one, the intermediate nodes adds its IP address to the route request and relay the request, so that when query packets arrive at the destination, only a limited amount of state information are needed to be maintained regarding the relayed queries, thus previously seen route requests are discarded at the destination. When route requests reach the destination T, T verifies the request. Then T constructs a route replies and calculates a MAC covering the route reply contents and returns the packet to S over the reverse of the route accumulated in the respective request packet.

The SRP uses an additional header called SRP header to the underlying routing protocol (e.g. AODV) packet. SRP header contains the following fields: the query sequence number QSEC, query identifier number QID, and a 96 bit MAC field. Intermediate nodes discard a route request message if SRP header is missing. Otherwise, they forward the request towards destination after extracting QID, source, and destination address. Highest priority is given to nodes that generate requests at the lowest rates and vice versa. When the target T receives this request packet, it verifies if the packet has originated from the node with which it has SA. If QSEC is greater or equal to QMAX, the request is dropped as it is considered to be replayed. Otherwise it calculates the keyed hash of the request fields and if the output matches SRP MAC then authenticity of the sender and integrity of the request are verified.

On the reception of a route reply, S checks the source address, destination addresses, QID, and QSEC. It discards the route reply if it does not match the currently pending query. In case of a match, it compares reply IP source- route with the exact reverse of the route carried in reply packet. If the two routes match then S calculates the MAC by using the replied route, the SRP header fields, and the secure key between source and destination. If the two MAC match then the validation is successful and it confirms that the reply did came from the destination T.

The drawback of SRP suffers from the lack of validation mechanism for route maintenance messages as it does not stop a malicious node from harming routes to which that node already belongs to. SRP is immune to IP spoofing because it secures the binding of the MAC and IP address of the nodes but it is prone to wormhole attacks and invisible node attacks. The basic version of SRP suffers from the route cache poisoning attack. SRP suffers from the lack of a validation mechanism for route maintenance messages. SRP is not immune to the wormhole attack: two colluding malicious nodes can misroute the routing packets on a private network connection and alter the perception of the network topology by legitimate nodes.

Strengths of SRP, It copes with non-colluding malicious nodes that are able to modify (corrupt), replay and fabricate routing packets. Assuming that the neighbour discovery mechanism maintains information on the binding of the medium access control and the IP addresses of nodes, SRP is proven to be essentially immune to IP spoofing. In case of the Dynamic Source Routing (DSR) protocol, SRP requires including a 6-word header containing unique identifiers that tag the discovery process and a message authentication code (MAC) computed using a keyed hash algorithm [8][9].

A Secure Routing Protocol for Ad Hoc Networks (ARAN)

ARAN is an on- demand protocol designed to provide secure communications in managed- open environments. Nodes in a managed-open environment exchange initialization parameters before the start of communication. Session keys are exchanged or distributed through a trusted third party like a certification authority. The ARAN secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the ad hoc environment and consists of a preliminary certification process, a mandatory end to-end authentication stage and an optional second stage that provides secure shortest paths. Using pre-determined cryptographic certificates, ARAN provides network services like authentication and non-repudiation. Simulations show that ARAN is efficient in discovering and maintaining routes but routing packets are larger in size and overall routing load is high. Due to heavy asymmetric cryptographic computation, ARAN has higher cost for route discovery. It is not immune to wormhole attack and if nodes do not have time synchronization, then it is prone to replay attacks as well.

ARAN requires the use of a trusted certificate server (T): before entering in the ad hoc network, each node has to request a certificate signed by T. The certificate contains the IP address of the node, its public key, a timestamp of when the certificate was created and a time at which the certificate expires along with the signature by T. All nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key. The goal of the first stage of the ARAN protocol is for the source to verify that the intended destination was reached. As with any secure system based on cryptographic certificates, the key revocation issue has to be addressed in order to make sure that expired or revoked certificates do not allow the holder to access the network. In ARAN, when a certificate needs to be revoked, the trusted certificate server T sends a broadcast message to the ad hoc group that announces the revocation. Any node receiving this message rebroadcasts it to its neighbours. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbour of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un-trusted node. This method is not failsafe. In some cases, the un-trusted node that is having its certificate revoked may be the sole connection between two parts of the ad hoc network. In this case, the non- trusted node might not forward the notice of revocation for its certificate, resulting in a partition of the network, as nodes that have received the revocation notice will no longer forward messages through the un-trusted node, while all other nodes depend on it to reach the rest of the network. This only lasts as long as the un-trusted node's certificate would have otherwise been valid, or until the un-trusted node is no longer the sole connection between the two partitions. At the time that the revoked certificate should have expired, the un-trusted node is unable to renew the certificate, and routing across that node ceases. Additionally, to detect this situation and to hasten the propagation of revocation notices, when a node meets a new neighbour, it can exchange a summary of its revocation notices with that neighbour; if these summaries do not match, the actual signed notices can be forwarded and re-broadcasted to restart propagation of the notice [10][11].

Security Aware Routing (SAR)

Security Aware Routing (SAR) is an on demand routing protocol implemented over AODV. It integrates the trust level of a node and the security attributes of a route to provide an integrated security metric for the requested route. By incorporating a Quality of Protection (QoP) as a routing metric, the route discovery can return quantifiable secure routes. The QoP vector used is a combination of security level and available cryptographic techniques SAR introduces the notion of a trust hierarchy, where nodes of the ad hoc wireless network are divided into different trust levels such that an initiator can impose a minimum trust level for all the nodes participating in the source-destination communication. Note that a path with the required trust level might not exist even if the network is connected. Even if SAR discovers fewer routes than AODV, they are always secured.

AODV is a reactive distance vector routing protocol. A route is discovered only when necessary. To request a route, source node broadcasts a Route Request message (RREQ), which has a unique sequence number. When the RREQ message reaches either the destination or an intermediate node that has a valid route to the destination, a Route Reply message (RREP) is created and unicasted back to the source node. As the RREP propagates back to the source, intermediate nodes receiving the RREP update their routing tables with a route to the destination.

SAR when implemented on AODV protocol adds two additional fields to the Route Request packet and one additional to the Route Reply packet. The first field added to the Route Request packet is the security requirement field and is set by the sender .It indicates the preferred level of trust for the path to the destination. The Second field added to is the security guarantee that signifies the maximum level of security provided by the discovered paths. If the security requirement field has an integer representation then the security guarantee field will be minimum of all security levels of the participating nodes in the path. If the security requirement field is represented in vectors then the security guarantee field value is computed by adding the security requirement values of the participating nodes in the path. The value thus computed is copied into additional security guarantee field of the Route Reply packet and sent back to the sender. This value is also copied into the routing table of nodes in the reverse path, to preserve the security information with reference to cashed paths

The fewer advantage of SAR uses security information to dynamically control the choice of routes installed in the routing table. (ii) SAR enables applications to selectively implement a subset of security services based on the cost-benefit analysis. (iii) The routes discovered by SAR may not always be the shortest between any two communicating entities in terms of hop count. However these routes have quantifiable guarantee of the security. (iv) SAR will find the

optimal route if all the nodes on the shortest path satisfy the security requirements. (v) SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected [12].

ARIADNE

It is an efficient on-demand secure routing protocol, provides security against arbitrary active attackers and relies only on efficient symmetric cryptography. It prevents attackers from tampering uncompromised routes consisting of uncompromised nodes. ARIADNE ensures point-to-point authentication of a routing message by combining a shared key between the two parties and MAC.

Design of ARIADNE is based on DSR . Similar with DSR, it consists of two basic operations, route discovery and route maintenance. ARIADNE makes use of efficient combination of one way hash function and shared keys. It assumes that sender and receiver share secret keys for message authentication. The initiator (or sender) includes a MAC computed with an end-to-end key and the target (or destination) verifies the authenticity and freshness of the request using the shared key. Pre-hop hashing mechanism, a one-way hash function that verifies that no hop is omitted, is also used in Ariadne. In the case of any dead link, a RouteError message is sent back to the initiator. Errors are generated just as regular data packets and intermediate nodes remove routes that use dead links in the selected path [13][14].

Secure Efficient Ad hoc Distance Vector (SEAD)

Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of DSDV . Besides the fields common with DSDV, such as destination, metric, next hop and sequence number, SEAD routing tables maintain a hash value for each entry, as described below. This paper is concerned with protecting routing updates, both periodic and triggered, by preventing an attacker to forge better metrics or sequence numbers in such update packets. The key feature of the proposed security protocol is the use one-way hash chains, using an one way hash function H. Each node computes a list of hash values h0, h1, ・ ・ ・ , hn, where hi = H(hi−1) and 0 < i ≤ n, based on an initial random value h0. The paper assumes the existence of a mechanism for distributing hn to all intended receivers. If a node knows H and a trusted value hn, then it can authenticate any other value hi, 0 < i ≤ n by successively applying the hash function H and then comparing the result with hn.

To authenticate a route update, a node adds a hash value to each routing table entry. For a metric j and a sequence number i, the hash value hn−mi+j is used to authenticate the routing update entry for that sequence number, where m − 1 is the maximum network diameter. Since an attacker cannot compute a hash value with a smaller index than the advertised value, he is not able to advertise a route to the same destination with a greater sequence number, or with a better metric.

SEAD provides a robust protocol against attackers trying to create in- correct routing state in other node by modifying the sequence number or the routing metric. SEAD does not provide a way to prevent an attacker from tampering next hop or destination field in a routing update. Also, it cannot prevent an attacker to use the same metric and sequence number learned from some recent update message, for sending a new routing update to a different destination.

(i) SEAD deals with attackers that modify routing information broadcasted during the update phase of the DSDVSQ protocol in particular, routing can be disrupted if the attacker modifies the sequence number and the metric field of a routing table update message.

(ii) SEAD makes use of efficient one-way hash chains rather than relying on expensive asymmetric cryptography operations.

(iii) SEAD assumes some mechanism for a node to distribute an authentic element of the hash chain that can be used to authenticate all the other elements of the chain.

(d) Weakness SEAD does not cope with wormhole attacks [15].

Cooperation Of Nodes Fairness In Dynamic Ad-hoc Networks (CONFIDANT)

Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) [2] protocol is designed as an extension to reactive source-routing protocol such as DSR. It is a collection of components which interact with each other for monitoring, reporting, and establishing routes by avoiding misbehaving nodes. CONFIDANT components in each node include a network monitor, reputation system, trust manager, and a path manager.

Each node in this protocol monitors their neighbors and updates the reputation accordingly. If they detect any misbehaving or malicious node, they can inform other friend nodes by sending an ALARM message. When a node receives such an ALARM either directly from another node or by listening to the ad hoc network, it calculates how trustworthy the ALARM is based on the source of the ALARM and the total number of ALARM messages about the misbehaving node.
Trust manager sends alarm messages to other nodes to warn them of malicious nodes. Incoming alarms are checked for trustworthiness. Trust manager contains an alarm table, trust level table and a friend list of all trust worthy nodes to which a node will send alarms.

Local rating lists and black lists are maintained in the reputation system. These lists are exchanged with friend nodes and timeouts are used to avoid old lists. A node gives more importance to its own experience than to those events which are observed and reported by others. Whenever the threshold for certain behavior is crossed, path manager does the re-ranking by deleting the paths containing malicious nodes and ignoring any request from misbehaving nodes. At the same time, it sends an alert to the source of the path so that it can discover some other route. When DSR is fortified with the CONFIDANT protocol extensions, it is very scalable in terms of the total number of nodes in the network and it performs well even if more than 60% of the nodes are

misbehaving. The overhead for incorporating different security components is manageable for ad hoc environment. However, detection based reputation system has few limitations and routes are still vulnerable to spoofing and Sybil attacks [16].

Defense Operations from Rushing Attacks

Rushing attacks are mostly directed against on demand routing protocols such as DSR. To counter such attacks, a generic secure route discovery component called Rushing Attack Prevention (RAP) is used. RAP combines the following mechanisms: Secure Neighbor Detection, Secure Route Delegation, and Randomized Route Request Forwarding. Any on demand routing protocol such as ARIADNE can be used as underlying protocol to RAP [17] .

In ***Secure Neighbor Detection***, a three round mutual authentication procedure is used between a sender and a receiver to check if they are within normal communication range of each other. First, a node forwards a Neighbor Solicitation packet to the neighboring node which replies with a Neighbor Reply packet and finally, the initial node sends Neighbor Verification packet to confirm that both nodes are neighbors.

Secure Route Delegation verifies that all the steps in Secure Neighbor Detection phase were carried out. Before sending a route update to its neighbor, it signs a route attestation, delegating the rights to the neighbor to further propagate the update.

In ***Randomize Message Forwarding***, a node buffers k route requests and then it randomly forwards only one of these k requests. By limiting the total number of requests sent by a node, it prevents flood attacks in the network. Each request carries the list of all the nodes traversed by that request. Furthermore, bi-directional verification is also used to authenticate the neighbors. By using efficiently combining these three mechanisms, RAP can find usable routes when other protocols cannot. When it is enabled, it has higher overhead than other protocols, but currently it is the only protocol that can defend against rushing attacks. However, network is still prone to rushing attacks if an attacker can compromise k nodes.

Defense Operations from Wormhole Attacks

In order to prevent the wormhole attacks the packet leashes mechanism proposes to add additional information to the packets in order to restrict packet's maximum allowed transmission distance. Geographical leash and temporal leash can be used to detect and stop wormhole attacks. Geographical leash insures that the recipient of the packet is within a certain distance from the sender while temporal leash is used to enforce an upper bound on the packet's life time, thus restricting packet's maximum travel distance. Temporal leash uses packet's expiration time to detect a wormhole. The expiration time is computed based on the allowed maximum transmission distance and the speed of light. A node will not accept any packet if this expiration time has passed. TIK (TESLA with Instant Key Disclosure) protocol is an extension of TESLA and it is implemented with temporal leashes to detect wormholes. It requires each communicating node to know one public key for each other node in the network [18].

Defense Operations from Sybil Attacks

Sybil attack is a malicious node acts on behalf of a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Most of the secure protocols are prone to this type of attack. However, there are various key distribution mechanisms which can be used efficiently to defend against Sybil attacks. Sybil nodes can carry out a variety of attacks. For example, network nodes use voting for many purposes. With enough Sybil nodes, an attacker may be able to determine the outcome of every vote. Sybil nodes, due to their larger number, are allocated more resources and they can create DoS for legitimate nodes. Ad hoc wireless networks can use misbehavior detection property to detect any malfunctioning node. An attacker with many Sybil nodes can spread the blame and pass unnoticed, having only small misbehavior actions associated with each identity.

There are a number of ways to detect Sybil attacks. In radio resource testing, it is assumed that nodes have only one radio and are not capable of sending or receiving on more than one channel. If a node wants to verify whether its neighbors are Sybil nodes, then it assigns to each of its neighbors a different channel to broadcast messages. Then the node listens to one of the channels. If a message is received, this is an indication of a legitimate neighbor, whereas an idle transmission is an indication of a Sybil node. A more authentic way of defending against Sybil attacks is random key predistribution. A random set of keys are assigned to each node and then every node can compute the common keys it shares with its neighbors [19].

Security from Broadcast Operation

Timed Efficient Stream Loss-tolerant Authentication (TESLA) [20] is an efficient broadcast authentication protocol with low communication and computation overhead. It can scale to large numbers of receivers, can tolerate packet loss, and uses loose time synchronization between sender and receivers. TESLA mainly uses purely symmetric cryptographic functions, however, it achieves asymmetric properties from clock synchronization and delayed key disclosure. In this way, it does not require to compute expensive one way functions. For this purpose, it needs sender and receivers to be loosely time-synchronized and for a secure authentication, either the receiver or the sender must buffer some messages.

IV. CONCLUSION

Accomplish the secure routing protocols are an important role that is being challenged by the unique characteristics of wireless ad hoc network. Usual routing protocols not succeed to give security, and rely on an understood confidence between communicating nodes. In this paper we discuss security services and challenges in an ad hoc wireless network environment. We observe and categorize major routing protocols working against attacks.

V.REFERENCE

[1] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Kluwer Academic Publishers, Vol 353, 1996, pp. 153-181.

[2] Huaizhi Li et al Secure Routing in Wired Networks and Wireless Ad Hoc Networks, Department of Computer Science University of Kentucky, April, 2002

[3] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.

[4] Y. -C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Infocom 2003.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding Royer, A Secure Routing Protocol for Ad hoc Networks, The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.

[6] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[7] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, 2003.

[8] Panagiotis Papadimitratos and Zygmunt Haas. Secure Routing for Mobile
Ad hoc Networks. In Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.

[9] P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad hoc Networks, In Proc. of the SCS Communication Networks and Distributed
Systems Modeling and Simulation Conference (CNDS 2002), Jan. 2002.

[10] Bridget Dahill, Brian Levine, Elizabeth Royer, and Clay Shields. A Secure Routing Protocol for Ad Hoc Networks. Technical Report UM-CS-2001- 037, University of Massachusetts, August 2001.

[11] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, A Secure Routing Protocol for Ad hoc Networks, The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.

[12] R. Kravets, S. Yi, and P. Naldurg, A Security-Aware Routing Protocol for Wireless Ad Hoc Networks, In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.

[13] Y. -C. Hu, D. B. Johnson, and A. Perrig, Ariadne: A Secure On-Demand
Routing Protocol for Ad Hoc Networks, Mobicom'02, 2002.

[14] Yih-Chun Hu, David B. Johnson, and
Adrian Perrig. Secure On-Demand Routing Protocols in Ad Hoc Networks. Unpublished, 2001.

[15] Yih-Chun Hu, David Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In Workshop on Mobile Computing Systems and Applications. IEEE, June 2002.

[16] S. Buchegger and J. L. Boudec, Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks, In Proc. of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Jun. 2002.

[17] Y. -C. Hu, D. B. Johnson, and A. Perrig, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, 2003.

[18] Y. -C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Infocom 2003.

[19] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.

[20] A. Perrig, R. Canetti, D. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories), Vol 5, No 2, Summer/Fall 2002, pp. 2-13.

Authors Profile

K.S.Saravanan received his M.Phil(C.S) Degree from Periyar University in the year 2008. He has received his M.C.A, Degree from Bharadhiar University, Coimbatore in the year 2000. He is working as Assistant Professor, Department of Computer Application, Vivekanandha College of Arts and Science for Women, Namakkal, Tamilnadu, India. His areas of interest include Networking , Ad hoc Network and Wireless Sensor Networks.

Dr.N.Rajendran received his Ph.D Degree from Periyar University, Salem in the year 2011. He has received his M.Phil, Degree from Bharathiar University, Coimbatore in the year 2000. He has received his M.C.A Degree from Madras University, Chennai in the year 1990. He is working as Principal of Vivekanandha Arts and Science College for Women, Sankari, Salem , Tamilnadu, . He has 24 years of experience in academic field. He has published 18 International Journal papers and 19 papers in National and International Conferences. His areas of interest include Digital Image Processing and Networking.