International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 5– No.4, March 2013 – www.ijais.org

Survey - Secure Routing Protocols of MANET

Jayashree.A.Patil
Asst.Prof.Department of Information Technology
MIT Academy of Engineering Alandi (D), Pune

Nandini Sidnal, Ph.D.
Head, Department of Computer Science and Engineering
KLE's MSSCOET, Belgaum

ABSTRACT

Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node not only acts as end system, but also as a router to forward packets. The nodes are free to move and organize themselves and change topology dynamically, establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. But one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. As a result, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to cripple the MANET operations. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks**.** Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security plays an important role the network (MANET). In this paper, we identify the existent security threats where an ad hoc network faces,and some of the issues and challenges of MANET, we have done literature survey and gathered information related to various types of attacks and solutions.

However in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

General Terms

Security, Algorithms, Protocols.

Keywords

MANET, Attacks, AODV, DSR.

1. INTRODUCTION

We are living in the information age. Information is an asset that has a value like any other assets. As the information is distributed, information needs to be secured from attacks and needs to be hidden from confidentiality, integrity and availability.A number of attacks in different layers are identified and studied in research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. So special routing algorithms are needed. There is no single protocol that fits all networks perfectly. The protocols have been chosen according to network characteristics such as density, size and mobility of nodes. There is still ongoing research on mobile ad hoc networks and research may lead to even better protocols and will probably face new challenges.

Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic. This assumption can prove to be disastrous for an ad hoc network that relies on intermediate nodes for packet forwarding. Earlier surveys and review papers presenting comparisons of ad hoc routing protocols completely ignored security problems [2, 3]. This article presents a survey of the solutions that address the problem of secure and robust routing in mobile ad hoc networks. The paper is organized as follows.

Section II deals with security problems and different attacks of each layer. Section III explores about some of the existing secure routing protocols. In section III Comparison is made among different existed protocols a And the paper ends with Conclusion.

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. These vulnerabilities can be challenges and issues of MANET security. Some of the vulnerabilities are as follows:-

1. Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

2. Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3. Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4. Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

5. Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

6. Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

7.Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

8. No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack.

SECTION II- SECURITY PROBLEMS WITH EXISTING AD HOC ROUTING PROTOCOLS

MANET is infrastureless network there is huge chance of security attacks. There exist three main security goals they are. Confidentiality, integrity and availability. Attacks threatening confidentiality are Snooping: snooping refers to unauthorized access to or interception of data [1]. Traffic analysis: anybody can obtain some other type of information by monitoring online traffic**.** The integrity of data can be threatened by several kinds of attacks: modification, masquerading, replaying, repudiation. The availability of data can be threatened by Denial of Services [1].

Based on the threat analysis and the identified capabilities of the potential attackers, we will now discuss several specific attacks that can target the operation of a routing protocol in an ad hoc network.

Location Disclosure: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [12], or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network. **[11]**

Black Hole: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets **[9]**.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions **[7]**.

Wormhole: The wormhole attack is one of the most powerful since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers **[13]**.

Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network **[14]**. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [15].

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow [11] and the sleep deprivation torture [16]. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Routing Table Poisoning: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even partitioning certain parts of the network.

SECTION III - SECURE AD HOC ROUTING

There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned in the previous section. These proposed solutions are either completely new stand-alone protocols, or since routing is an essential function of ad hoc networks, the integrated security procedures should not hinder its operation.

Authenticated Routing for Ad hoc Networks (ARAN)

The Authenticated Routing for Ad hoc Networks (ARAN) protocol, proposed in [17], is a stand-alone solution for securing routing in ad hoc networking environments. ARAN utilizes cryptographic certificates in order to achieve the security goals of authentication and non-repudiation. ARAN, an on-demand secure ad hoc routing protocol, consists of three distinct operational stages, of which the first two are compulsory and the third is optional. The first stage is, in essence, a preliminary certification process that requires the existence of a trusted certification authority (CA). **The protocol assumes that each node knows a priori the public key of the certification authority**. The second operational stage of the protocol is the route discovery process that provides end-to-end authentication. This ensures that the intended destination was indeed reached. Each node must maintain a routing table with entries that correspond to the source-destination pairs that are currently active. The ARAN protocol does not allow intermediate nodes that have paths to a destination to reply to a route discovery packet. This guarantees that only the destination can answer a route discovery, thus ensuring loop freedom but at the cost of high latency [17].

The third operational stage of the ARAN protocol is optional and ensures that the shortest paths are discovered. However, this optimization comes at a high cost. The ARAN protocol requires a trusted certification authority to exist in the ad hoc network in order to authenticate routing traffic. Authentication in ARAN is provided through public key cryptography. Routing traffic messages, such as route discoveries and route replies, must be signed by the node that generates or forwards them.

Secure Efficient Ad hoc Distance Vector Routing (SEAD) — The Secure Efficient Ad hoc Distance vector (SEAD) is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithm [14]. In order to find the shortest path between two nodes, the distance vector routing protocols utilize a distributed version of the Bellman-Ford algorithm [5]. The SEAD routing protocol employs the use of hash chains to authenticate hop counts and sequence numbers. Applying repeatedly a one-way hash function to a random value creates a hash chain. The elements of such a chain are used to secure the updates of the routing protocol. SEAD requires the existence of an authentication and key distribution scheme in order to authenticate one element of a hash chain between two nodes.

Secure Routing Protocol (SRP) — The Secure Routing Protocol (SRP) is a set of security extensions that can be applied to any ad hoc routing protocol that utilizes broadcasting as its route querying method [18]. The authors specifically mention DSR as a particularly appropriate protocol for incorporating their proposed security extensions. The operation of SRP requires the existence of a security association (SA) between the source node initiating a route query and the destination node. This security association can be utilized in order to establish a shared secret key between the two, which is used by SRP.

The SRP protocol appends a header (SRP header) to the packet of the basis routing protocol. The source node sends a route request with a query sequence (QSEQ) number that is used by the destination in order to identify outdated requests, a random query identifier (QID) that is used to identify the specific request, and the output of a keyed hash function.SRP consists of several security extensions that can be applied to existing ad hoc routing protocols providing end-to end authentication. The operational requirement of SRP is the existence of a security association between every source and destination node. The security association is used to establish a shared secret between the two nodes, and the non mutable fields of the exchanged routing messages are protected by this shared secret.

Ariadne — Ariadne is a secure on-demand ad hoc routing protocol based on DSR and developed by the authors of the SEAD protocol. Security in Ariadne follows an end-to-end approach, while the SEAD protocol employs hop-by-hop security mechanisms due to the distance vector routing philosophy it adopts. Ariadne assumes the existence of a shared secret key between two nodes, and uses a message authentication code (MAC) in order to authenticate point-to-point messages between these nodes [20]. Additionally, Ariadne employs the TESLA broadcast authentication protocol to authenticate broadcast messages, such as route requests. In TESLA a sender generates a one way key chain and defines a schedule according to which it discloses the keys of the chain in reverse order from generation [19]. Therefore, time synchronization is an absolute requirement of ad hoc networks that use Ariadne.

The Ariadne protocol also specifies a mechanism for securing route maintenance, which ensures the validity of route error messages concerning broken links in the ad hoc network. Ariadne is based on DSR and provides end-to-end security mechanisms for ad hoc routing. Ariadne utilizes a message authentication code in order to authenticate routing table entries. The most important requirement of Ariadne is the existence of clock synchronization in the ad hoc network. The basic Ariadne protocol can be disrupted by wormhole attacks, but an extension developed by the authors can be utilized to secure against it [21].

Secure Ad hoc On-demand Distance Vector Routing (SAODV) — Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol [22]. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets. In particular, cryptographic signatures are used for authenticating the non-mutable fields of the messages, while a new one way hash chain is created for every route discovery process to secure the hop-count field, which is the only mutable field of an AODV message. Since the protocol uses asymmetric cryptography for digital signatures it requires the existence of a key management mechanism that enables a node to acquire and verify the public key of other nodes that participate in the ad hoc network.

Secure Link State Routing Protocol (SLSP) — The Secure Link State Routing Protocol (SLSP) [23] has been proposed to provide secure proactive routing for mobile ad hoc networks. It secures the discovery and the distribution of link state information both for locally and network-wide scoped topologies. SLSP can be employed as a stand-alone solution for proactive link-state routing, or combined with a reactive ad hoc routing protocol creating a hybrid framework. The main operational requirement of SLSP is the existence of an asymmetric key pair for every network interface of a node. Participating nodes are identified by the IP addresses of their interfaces. The specific mechanism for the certification of public keys is not addressed by the protocol, as previously proposed key management solutions are assumed to be in operation. Furthermore, SLSP limits its scope to secure only the process of topology discovery; parties that participate in it and decide to misbehave during data transmission are not detected or penalized. SLSP can be logically divided into three components: public key distribution, neighbor discovery, and link state updates. SLSP provides a proactive secure link state routing solution for ad hoc networks. As mentioned by the authors, SLSP is vulnerable to colluding attackers that fabricate non-existing links between themselves and flood this information to their neighboring nodes.

On-demand Secure Routing Protocol Resilient to Byzantine Failures (OSRP) — The problem of malicious nodes in an ad hoc network performing byzantine attacks in order to disrupt the routing function is studied in [10]. The authors propose an on-demand secure routing protocol that is able to function in the presence of colluding nodes introducing byzantine failures in the process of routing. Their approach is based on the detection of faulty links after log n faults have occurred, where n is the length of the route. The protocol bases on demand route discovery on weight values of paths, and the paths that are identified as malicious are assigned increased weights. The authors define the term byzantine behavior as any action taken by an authenticated node that disrupts the routing process.

The protocol is separated into three different phases: route discovery with fault avoidance, byzantine fault detection, and link weight management. The phases operate in sequence and each one receives the output of the previous as input .The metric upon which path selection is based consists of link weights, where high weights represent an unreliable path. Every node that participates in the network is required to maintain a weight list and update it according to the results of the fault detection phase. The first phase of the protocol is responsible for establishing a route between the initiating and the destination node. The initiating node signs with its private key a route request message that is broadcast to all of its neighbors. The message includes the address of the initiator, the address of the destination, a sequence number, and a weight list. The second phase of the protocol, byzantine fault detection, requires specific nodes on a discovered path to return Acknowledgments to the source node. Data packets originating from the source contain a list of nodes, known as probe nodes, which are required to send Acknowledgments for every received packet. If the number of unacknowledged packets violates an acceptable threshold, a fault is registered on the path. Thus, a malicious node is not able to drop packets without actually dropping the list of the probe nodes. The list contains non-overlapping intervals that cover a route, where each interval covers the sub-path between two consecutive nodes [10]. Using binary search, the fault detection algorithm is able to locate a faulty link after log n faults have been detected, where n is the length of the route where a fault was registered. The main goal of the protocol is to provide a robust on demand ad hoc routing service that is resilient to byzantine failures. The operation of the protocol requires the existence of public-key infrastructure in the ad hoc network to certify the authenticity of the participating nodes' public-keys. Based on this assumption, the protocol manages to discover a fault free path if one exists even in an environment with colluding malicious nodes. As the authors note, a limitation rests in the inability of the protocol to prevent wormhole attacks. However, if the wormhole link demonstrates byzantine behavior then the protocol will detect it and avoid it [10].

Watchdog and Pathrater — The watchdog and pathrater scheme consists of two extensions to the DSR routing protocol that attempt to detect and mitigate the effects of nodes that do not forward packets although they have agreed to do so [2]. This misbehavior may be due to malicious or selfish intent, or simply the result of resource overload. Although the specific methods proposed build on top of DSR, the authors suggest that the basic concepts can be applied to other source routing protocols for ad hoc networks. The watchdog extension is responsible for monitoring that the next node in the path forwards data packets by listening in promiscuous mode. It identifies as misbehavior nodes those nodes that fail to do so. The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. One of the base assumptions of this scheme is that malicious nodes do not collude in order to circumvent it and perform sophisticated attacks against the routing protocol. The watchdog of a node maintains copies of recently forwarded packets and compares them with the packet transmissions overheard by the neighboring nodes. Positive comparisons result in the deletion of the buffered packet and the freeing of the related memory. If a node that was supposed to forward a packet fails to do so within a certain timeout period, the watchdog of an overhearing node increments a failure rating for the specific node. This effectively means that every node in the ad hoc network maintains a rating assessing the reliability of every other node from which it can overhear packet transmissions. A node is identified as misbehaving when the failure rating exceeds a certain threshold bandwidth [2]. The source node of the route that contains the offending node is notified by a message sent by the identifying watchdog. As the authors of the scheme note, the main problem with this approach is its vulnerability to blackmail attacks. The pathrater extension to DSR selects routes for packet forwarding based on the reliability rating assigned by the watchdog mechanism. it suffers from the possibility of blackmail attacks.

CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)- CONFIDANT protocol consists of a set of extensions to DSR that include the following components: the monitor, the reputation system, the path manager, and the trust manager [24]. A node that participates in the protocol must operate all four components. Routing paths are chosen based on ratings assigned through directly observed or reported routing and forwarding behavior. The monitor component of a CONFIDANT node is responsible for monitoring passive acknowledgments for each packet it forwards. This is similar to the watchdog functionality that we discussed in the previous paragraph. It is important to note that the CONFIDANT protocol only supports the building of negative experiences associated with a node identity. Each entry in the list of identified attackers maintained by a node is associated with a timer. When this expires the entry is purged and the node is again considered to be a legitimate participant of the ad hoc network.

Security-aware Ad hoc Routing (SAR) — Security-aware Ad hoc Routing (SAR), described in [25], is an approach to ad hoc routing that introduces a security metric in the route discovery and maintenance operations, treating secure routing as a quality of service (QoS) issue. While traditional non secure routing protocols utilize distance (measured in hop counts), location, power, and other metrics for routing decisions, SAR uses security attributes (such as trust values and trust relationships) in order to define a routing metric. Its operation is applicable in situations where a route that satisfies certain security requirements is more important than a route that satisfies any other requirement. SAR extends on-demand ad hoc routing protocols (such as AODV or DSR) in order to incorporate the security metric into the route request messages. The authors present an implementation of SAR based on AODV, which they call SAODV (Security-aware AODV). The initiator broadcasts a route request

(RREQ) with an additional field (RQ_SEC_REQUIREMENT) that indicates the required security level of the route that she wishes to discover [37]. A neighboring node that receives the packet checks whether it can satisfy the security requirement. If the node can provide the required security then it can participate in the requested route and re-broadcasts the packet to its own neighbors, setting a new field called RQ_SEC_GURANTEE to indicate the maximum level of security it can provide. If a node is not secure enough to participate in the requested route, it simply drops the RREQ. Therefore, when the destination node receives the RREQ it can be sure that a route to the source node exists and that this route satisfies the security requirements defined by the initiator. The destination sends a route reply (RREP) packet with an additional field (RP_SEC_GUARANTEE) that indicates the maximum level of security of the found route. The RREP message travels back along the reverse path of the intermediate nodes that were allowed to participate in the routing, and each node updates its routing table according to the AODV specification, including the RP_SEC_GUARANTEE value. This value is used in order to allow intermediate nodes with cached routes to reply to a request of a route with a specific security requirement. The security metric of SAR can be specified by hierarchies of trust levels or by desirable security properties. In order to define trust levels, a key distribution or secret sharing mechanism is required. By utilizing this mechanism all the nodes that belong to a particular trust level can share a key. Therefore, nodes of different security levels cannot decrypt or process routing packets and are forced to drop them. Furthermore, the security metric can be specified by standard security properties such as timeliness, ordering, and authenticity, to name a few [25]. These properties can be implemented in the SAR protocol by utilizing techniques such as timestamps, sequence numbers, and certificates, respectively.

However, each of these properties has a related cost and adds performance overhead to the routing process. Participating nodes can specify their exact security requirements based on security-performance trade-off decisions. The main idea behind SAR is the utilization of a security metric in place of the standard metrics, such as hop count, for the route discovery and maintenance functions. The security routing metric is defined through attributes that reflect certain security properties, such as authentication, non-repudiation, and others. Therefore, the discovered and maintained routes satisfy the requirements of the security metric.

Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA) — Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA) is a set of design techniques that can be applied on ad hoc routing protocols to mitigate the impact of malicious nodes and allow the acceptable operation of the network under denial of service attacks [26]. The design principles defined by TIARA can be incorporated more easily into on-demand routing protocols, such as DSR and AODV, and are enumerated here: flow-based route access control (FRAC), multi-path routing, source-initiated flow routing, flow monitoring, fast authentication, the use of sequence numbers and referral-based resource allocation.

TIARA provides general design principles and techniques that can be applied to existing ad hoc routing protocols to develop solutions resistant to denial of service attacks. The techniques provided by TIARA are protocol independent, but they require extensive changes to existing protocols in order to be successfully incorporated.

Building Secure Routing out of an Incomplete Set of Security Associations (BISS) — The protocols we have analyzed up to this point assume that a security association already exists between the initiator and the destination node, as with SRP, or that both the initiator and the destination must have established security associations with all the intermediate nodes on the routing path, as with Ariadne. The BISS protocol (Building Secure Routing out of an Incomplete Set of Security Associations) [27] is a set of optimizations to existing ad hoc routing protocols that have been designed with the assumption that participating nodes have established an incomplete set of security associations between themselves. The keys and certificates of previously The authentication of the intermediate nodes along a route discovery path is not performed only on the basis of pre established associations, but also by exchanging public key certificates with these nodes. BISS assumes that the target node of a route discovery process has an existing security association with the intermediate nodes and that an off-line trusted authority has certified the public keys of all the participating nodes.

Although the general ideas introduced by BISS can be applied to on-demand routing protocols, the authors have applied them to the DSR protocol. Route request packets are signed by the initiator and also include its public key and certificate. The certificate is signed by the trusted authority and binds the initiator's public key with an identifier, such as the node's address. The approach followed by BISS has the beneficial side effect of increasing the number of security associations in an unknown node are distributed in the network during the route discovery and allow nodes to establish symmetric shared secrets for using the keyed hash authentication method for future message verifications.

Packet Leashes — Packet leashes [21] are not a complete protocol but a specific solution than can be used in an existing protocol to protect against wormhole attacks. The main idea of the solution is to add some extra information to each packet sent in order to allow a receiving node to determine if a packet has traversed an unrealistic distance. The authors have proposed two kinds of leashes: temporal and geographical. According to the temporal leashes scheme, a node adds an extremely precise timestamp to each outgoing packet. The receiver is then able to authenticate the traveled distance given the time taken and the fact that this distance is bounded by the speed of light. As is obvious, the temporal leashes solution requires extremely precise clock synchronization, in the order of hundreds of nanoseconds, between all participating nodes. In order to deal with the uncertainty associated with the transmission times of highly congested nodes, the authors propose the use of a threshold time synchronization error.

The second method of constructing packet leashes is with the use of geographical location information, provided by systems such as the Global Positioning System (GPS) [28], and loosely synchronized clocks. A timestamp and the location information of the sender are added to each outgoing packet. The receiver is then able to verify the distance traveled by the packet during the last hop. All the nodes of the ad hoc network must have appropriate hardware to track their location according to a unified scheme. Clock synchronization in this method does not need to be as precise as with the temporal method since the location information is also used in the calculation of the distance between the sender and receiver.

In general, packet leashes provide a complete solution to the problem of wormholes in mobile ad hoc networks. Their operational requirement is either extremely precise clock synchronization, or less rigidly synchronized clocks and the knowledge of geographical location.

IP-level Security (IPSec) — several authors have proposed the use of IPSec as the underlying security mechanism for providing authentication, integrity, and confidentiality in mobile ad hoc networks [6, 11, 29]. According to this approach the operation of the routing protocol relies for protection on the security infrastructure provided by the IPSec suite. IPSec consists of a set of protocols that provide security services at the Internet Protocol (IP) level. These protocols guarantee the secure transmission of data between two systems anywhere in a networked environment. The goal of IPSec is to provide integrity, confidentiality, and authenticity. Moreover, it should be as resistant as possible to traffic analysis, replay, and man-in-the-middle attacks. The IPSec protocol suite consists of three different protocols [30]. First, the encapsulating security payload (ESP) is added to an IP datagram and provides confidentiality, integrity, and authenticity of the transferred data. The authentication header (AH) is also added to an IP datagram and provides integrity and authenticity of the transmitted packets. AH does not provide confidentiality for the data of network packets since this is the service explicitly provided by ESP. The third protocol is the internet key exchange (IKE), which is the protocol that negotiates the security association between the two endpoints that need to communicate, exchanges the necessary cryptographic keys, and sets up the connection configuration parameters. A security installation based on IPSec requires either the existence of prearranged common secrets between each pair of systems that need to communicate, or an online trusted third party, e.g. a certification authority, in order to certify the validity of the signed Diffie-Hellman key exchange messages and guarantee the identity of the communicating end points. Unfortunately, neither of the above requirements can be realistically assumed in an ad hoc network. Furthermore, the approach of using IPSec as an underlying security solution has been criticized for producing additional configuration overhead [31]. Another consideration is that when a security solution is not designed concurrently with the basic protocol, but is applied afterward, it may leave unpredictable and undetectable vulnerabilities in the system. This is especially true in the case of IPSec as a retrofitted security solution, whose high level of complexity and lack of documentation hinders attempts at in-depth analysis [32]. Furthermore, even if IPSec can be employed to protect a routing protocol from external fabricated unauthorized traffic, it cannot guarantee correct operation under internal attacks [8].

Enhancing data security in ad hoc networks based on multipath routing

Because Ad hoc network characteristics (dynamic topology, infrastructure less, variable capacity links, etc.) are origins of many issues. Routing is an important aspect in ad hoc networks because of its special characteristics. Multiple disjointed paths can exist between nodes, thus multipath routing can be used to statistically enhance the confidentiality of exchanged messages between the source and destination nodes. Sending a confidential data on one path helps attackers to get the whole of data to secure easily. Whereas sending it in parts on different disjointed paths increases the confidentiality robustness because it is almost impossible to obtain all the parts of a message divided and sent on multiple paths existing between the source and the destination. Authors of the paper are interested in security based multipath routing protocols.

Multipath routing allows the establishment of multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing [18]. Multipath routing has been explored in several different contexts. Authors mentions, Advantage of using multipath routing improves ad hoc network security. Let us assume that there is a secret message, if it send it through a single path, the enemy can compromise it by compromising any one of the nodes along this path. However, if we divide it into multiple parts and send these multiple parts via multiple independent paths, then the enemy has to compromise all the pieces from all the paths to compromise the message[33].

SMT The Secure Message Transmission (SMT)

-- SMT scheme addresses data confidentiality, data integrity, and data availability in ad hoc network environment. The SMT scheme operates on an end-to end basis, assuming a Security Association (SA) between the source and destination nodes, thus, no link encryption is needed. This SA between end-nodes is used to provide data integrity and origin authentication, but it could also be utilized to facilitate end-to-end message encryption.

The scheme works on top of the existing secure routing protocols, which cannot be themselves ensure data security. SMT uses multipath routing to statistically enhance the confidentiality and availability of exchanged messages between the source and destination nodes. Whereas SPREAD was primarily designed with the confidentiality of data transmission in mind, the designers of SMT focused primarily on the reliability of data transmission. In SMT each path is continually given a reliability rating that is based on the number of successful and unsuccessful transmissions on that path. SMT uses these ratings in conjunction with a multipath routing algorithm to determine and maintain a maximally secure path set and adjust its parameters to remain efficient and effective. The SMT scheme proposes the use of an Information Dispersal Algorithm (IDA) [34] to divide messages into multiple pieces, each containing limited redundancy. Each piece is transmitted on a different node-disjointed path. A Message Authentication Code (MAC) is transmitted with each piece to provide data integrity and origin authentication. The information redundancy factor is the ratio N=M where any M out of N transmitted pieces is needed to reconstruct the original message. Note that, unlike the case with threshold secret sharing algorithms, it is not guaranteed that less than M pieces will not reveal any information about the original message.

Security Protocol for Reliable Data Delivery (SPREAD)

SPREAD scheme addresses data confidentiality and data availability in a hostile ad hoc environment. The confidentiality and availability of messages exchanged between the source and destination nodes are statistically enhanced by the use of multipath routing. At the source, messages are split into multiple pieces that are sent out via multiple independent paths. The destination node then combines the received pieces to reconstruct the original message. The SPREAD scheme assumes link encryption between neighboring nodes, with a different key used for each link. Thus, to compromise confidentiality of a secret message, an adversary has to collect and decrypt all pieces of the message. Since each piece takes a different independent path, an attacker should be present in multiple locations at the same time to overhear or intercept all of the pieces. The SPREAD scheme proposes the use of a .T; N/ threshold secret sharing algorithm [35] to divide messages into multiple pieces. A .T; N/ threshold secret sharing algorithm generates N pieces, called shares, such that the original message can be reconstructed from any T shares. So, using less than T shares cannot yield any information about the original message. SPREAD uses threshold secret sharing with multipath routing to achieve data optimal confidentiality.

Jigsaw Puzzle

The Jigsaw Puzzle scheme addresses data confidentiality and integrity in an ad hoc environment [36]. Multipath routing is used to statistically enhance the confidentiality of exchanged messages between the source and destination nodes. The All-or-Nothing Transform [37] is applied to a secret message to guarantee that no information can be obtained about the message unless all of its pieces are known. The message is then broken up into pieces by a jigsaw puzzle algorithm, which is based on operations with roots of polynomials. The pieces are transmitted across multiple node-disjointed paths. A Message Authentication Code (MAC) is transmitted with each piece to provide data integrity and origin authentication. Thus, it becomes impossible to compromise a secret message unless an adversary can eavesdrop close to the source or destination or simultaneously listen on all of the paths. In this method, the source and destination could share a secret prime number that could be used in the message division process. No data redundancy is provided by the scheme, so data availability may significantly suffer in the presence of node failures, topological changes, or active attacks. In fact, the lack of a data-availability mechanism reduces this scheme's effectiveness in a highly mobile and hostile environment. Compared proposed approaches to secure an ad hoc network (especially data confidentiality) using multiple existing paths. We can deduce, then, that securing efficiently an ad hoc network needs a robust solution that does not generate important overheads. We focus, in our solution, on securing flow transmissions in ad hoc networks. We exploit in our approach multipath existence to reinforce data confidentiality.

Securing data based multipath routing in ad hoc networks (SDMP)

The idea behind our protocol is to divide the initial message into parts then to encrypt and combine these parts by pairs. Then we exploit the characteristic of existence of multiple paths between nodes in an ad hoc network to increase the robustness of confidentiality. This is achieved by sending encrypted combinations on the different existing paths between the sender and the receiver. Even if an attacker succeeds to have one part or more of transmitted parts, the probability that the original message can be reconstructed is low. The originality of this approach is that it does not modify the existing lower layer protocols. Some assumptions should be taken into consideration, The sender `A' and the receiver `B' are authenticated, WEP or TKIP is used for the encryption/decryption of frames at MAC layer and the authentication of the terminals, A mechanism of discovering the topology of the network is available, The protocol uses a routing protocol supporting multipath routing.

CONCLUSION

In this paper all types of attacks and their solutions are discussed. And previously presented secure ad hoc routing protocols and some improvement over new protocols. Each protocol has a different set of operational requirements and provides protection against different attacks by utilizing particular approaches. Therefore, most of the protocols studied are related to AODV and DSR routing protocols. a detailed comparison can provide insight regarding the applicability of a particular protocol for a specific application domain. A security analysis is attempted focusing on the applicability of the previously described solution. The future scope of the paper is to more focus on Byzantine attacks and their routing protocols.

REFERENCES

[1] Behourouz Forouzan "Crytography and Network Security".

[2] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," Proc. 6th Annual ACM/IEEE Int'l. Conf MobileComp. and Net. (Mobicom'00), Boston, Massachusetts, Aug. 2000, pp. 255–65.

[3] S. Ramanathan and M. Steenstrup, "A Survey of Routing Techniques for Mobile Communications Networks," Mobile Networks And Applications, vol. 2, no. 1, Oct. 1996, pp. 89–104.

[4] T. Clausen, P. Jacquet, and L. Viennot, "Comparative Study of Routing Protocols for Mobile Ad hoc Networks," Med-Hoc- Net'02, Sardegna, Italy, Sept. 2002, p. 10.

[5] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector (DSDV) for Mobile Computers," Proc. ACM Conf. Commun. Architectures and Protocols (SIGCOMM' 94), London, UK, Aug. 1994, pp. 234–44.

[6] C. E Perkins, E. M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[7] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, Oct. 2002.

[8] P. Papadimitratos and Z. J. Haas, "Securing the Internet Routing Infrastructure," IEEE Commun. Mag., vol. 10, no. 40, Oct. 2002, pp. 60–68.

[9] R. Perlman, "Network Layer Protocols with Byzantine Robustness," Ph.D. Dissertation, MIT/LCS/TR-429, MIT, Oct. 1988.

[10] J. Lundberg, "Routing Security in Ad Hoc Networks," http://citeseer.nj.nec.com/400961.html.

[11] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," Proc. Wksp. Design

Issues in Anonymity and Unobservability, Berkeley, CA, July 2000, pp. 7– 26.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks,” Proc. 22nd Annual Joint Conf. IEEE Comp. and Commun. Societies (Infocom’03), San Francisco, CA, Apr. 2003.

[13] Y.-C. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc works,” Proc. 4th IEEE Wksp. Mobile Comp. Sys. and Applications, Callicoon, NY, June 2002, pp. 3–13.

[14] L. Zhou and Z. J. Haas, “Securing Ad hoc Networks,” IEEE Net. Mag., vol. 6, no. 13, Nov./Dec. 1999, pp. 24–30.

[15] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks,” Proc. 7th Int’l. Wksp. Security Protocols, Cambridge, UK, Apr. 1999, pp. 172–94.

[16] K. Sanzgiri et al., “A Secure Routing Protocol for Ad hoc Networks,” Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02), IEEE Press, 2002, pp. 78–87.

[17] S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks,” Proc. 2nd ACM Symp. Mobile Ad Hoc Net. and Comp. (Mobihoc’01), Long Beach, CA, Oct. 2001, pp. 299–302.

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks,”Proc. 22nd Ann. Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976–86.

[19] M. G. Zapata, and N. Asokan, “Secure Ad hoc On-demand Distance Vector Routing,” ACM Mobile Comp. and Commun.Review, vol. 3, no. 6, July 2002, pp. 106–07.

[20] R. Ramanujan, A. Ahamad, and K. Thurber, “Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA),” Proc.Military Commun. Conf. (MILCOM 2000), Los Angeles, CA, Oct. 2000, pp. 660–64.

[21] R. Ogier, M. Lewis, and F. Templin, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF),” Internet Draft,draft-ietf-manet-tbrpf-08.txt, Apr. 2003.

[22] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, Nov. 1998.

[23] K. Sufatrio and K.-Y. Lam, “Scalable Authentication Framework for Mobile IP (SAFE-MIP),” Internet Draft, draft-riomobileip-safe-mip-00.txt, Nov. 1999.

[24] T. Imielinski and J. C. Navas, “GPS-based Geographic Addressing, Routing, and Resource Discovery,” Commun. ACM, vol. 42, no. 4, Apr. 1999, pp. 86–92.

[25] S. Toner and D. O’Mahony, “Self-Organizing Node Address Management in Ad hoc Networks,” Pers. Wireless Commun., IFIP-TC6 8th Int’l. Conf. (PWC 2003), 2003, pp. 476–83. [26] S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks),” Proc. 3rd Symp. Mobile Ad Hoc Net. and Comp. (MobiHoc 2002), ACM Press, 2002, pp. 226–36.

[27] P. Papadimitratos and Z. J. Haas, “Secure Link State Routing for Mobile Ad hoc Networks,” Proc. IEEE Wksp. Security and Assurance in Ad hoc Networks, IEEE Press, 2003, pp. 27–31.

[28] S. Capkun and J.-P. Hubaux, “BISS: Building Secure Routing out of an Incomplete Set of Security Associations,” Proc. ACM Wksp. Wireless Security, ACM Press, 2003, pp. 21–29.

[29] B. Schneier, Applied Cryptography — Protocols, Algorithms and Source Code in C, 2nd Ed., John Wiley & Sons, Inc., 1996.

[30] D. Eastlake and P. Jones, “US Secure Hash Algorithm 1 (SHA1),” RFC 3174, Sept. 2001.

[31] R. Rivest, “The MD5 Message-Digest Algorithm,” RFC 1321, Apr. 1992.

[32] R. Resnick and R. Zeckhauser, “Trust Among Strangers in Internet Transactions: Empirical Analysis of Ebay’s Reputation System,” Advances in Applied Microeconomics: The Economics of the Internet and E-Commerce, vol. 11, Elsevier Science Ltd.,

[33] Jalel Ben Othman, Lynda Mokdad “Enhancing data security in ad hoc networks based on multipath routing”

[34] M.O. Rabin, “Efficient dispersal of information for security, load balancing and fault tolerance”, Journal of the ACM 36 (2) (1989) 335-348.

[35] A. Shamir, “How to share a secret, Communications of the ACM 22 (11) (1979)”, 612-613

[36] R.A. Vasudevan, S. Sanyal,” A novel multipath approach to security in mobile ad hoc networks”, in: International Conference Computers and Devices for Communication, Kolkata, India, Jan 2004.

[37] R.L. Rivest,” All-or-Nothing Encryption and the package Transform,” in: Fast Software Encryption Workshop, vol. 1267, Hafia, Israel, 1997, p. 210.