International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4502-4509 ISSN: 2249-6645

Security Attacks on Routing Protocols in Ad Hoc Wireless Networks

Simanta Sarma[1], Binita Devi[2]
[1](HOD & Asstt. Professor, Department of Computer Science, S.B.M.S College, Sualkuchi, Assam, India)
[2](Senior Faculty, Surojit Academy, Assam)

ABSTRACT: *In this Research paper we describe mobile ad hoc networking and Security Attacks on Routing Protocols in Ad Hoc Wireless Networks. Moreover we discuss Characteristics of differentiate ad hoc wireless networks and Problems about the routing protocols. We decisions of report Solutions for Routing Protocols in Ad Hoc Wireless Networks. This paper we discuss Security and protection of Aware Ad Hoc Routing. We discuss for another process of modification of Ad Hoc Wireless Networks and the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.*

KEY WORDS: *Mobile Ad Hoc Wireless Network, Security, routing protocols, SAR, Secure Routing, ARAN, CONFIDANT, SEAD.*

I. Introduction

Mobile Ad-hoc Networks are a collection of two or more devices equipped with wireless communications and networking Capability. These devices can communication with other nodes that immediately within their radio range. The nodes can be regarded as wireless mobile hosts with limited power and constrained bandwidth. For the later, the nodes should deploy an intermediate node to be the router to route the packet from the source toward the destination. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support modality and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure.

1.1. Characteristics of differentiate ad hoc wireless networks:

An ad hoc network has many characteristics that contrast sharply with fixed networks or last-hop wireless networks. First, there is no infrastructure support. All routers are mobile and can communicate with each other only when they are in transmission range. Second, ad hoc wirelesses nodes are resource constrained, with limited processing and memory capacity, and are usually powered with batteries. Finally, the communication medium in an ad hoc wireless network, i.e., radio waves, infrared, etc., can be easily eavesdropped. Hostile environments like battlefields or commando rescue operations are some of the important target application areas for ad-hoc wireless networks. We get the different types of characteristics of ad hoc networks. i.e.

1.1.1. Dynamic Network Topology:

This is triggered by node mobility, nodes leaving or joining the network, node inoperability due to the lack of power resources, etc. Nonetheless, the network connectivity should be maintained in order to allow applications and services to operate undisrupted.

1.1.2. Fluctuating Link Capacity:

The effects of high bit error rate are more profound in wireless communication. More than one end-to-end path can use a given link in ad hoc wireless networks, and if the link were to break, could disrupt several sessions during period of high bit transmission rate.

1.1.3. Distributed Operations

The protocols and algorithms designed for an ad hoc wireless network should be distributed in order to accommodate a dynamic topology and an infrastructure less architecture.

Wireless devices are battery powered, therefore there is a limited time they can operate without changing or replenish their energy resources. Designing energy efficient mechanisms are thus an important feature in designing algorithms and protocols.

II. Attacks on ad hoc wireless networks

In this paper we are concerned with security of routing protocols in ad hoc wireless networks. Routing is an important operation, providing the communication protocol for data delivery between wireless devices. Providing a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on ad hoc wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not.

1.2. Passive Attack

In passive attacks, an intruder the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect.

1.3. Active Attack:

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks.

1.3.1. External Attack

External Attacks are carried by nodes that are not legitimate part of the network. In external attacks, it is possible to disrupt the communication of an organization from the parking lot in front of the company office.

1.3.2.Internal Attack

Internal Attacks are from compromised nodes that were once legitimate part of the network. In ad hoc wireless network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.

III. Problems about the routing protocols

In this paper, we examine there are different types of problems about the routing protocols. i.e.

- First of all, consider the rapid passing pattern. We define the rapid passing pattern to be one node passing through the whole network very quickly. Such a rapid passing node will generate the following affects to the whole network. First, the topology of the network changed rapidly, which will lead to the lost of packets. Second, we have to modify every node's routing table that within the communication distance of the rapid-passing node, that will greatly improve the consumption of the bandwidth and the overhead of the networks. Third, obviously there will be tremendous delay of the data sending to the rapid-moving node.
- Transmission between two hosts over a wireless network does not necessarily work equally well in both directions. Thus, some routes determined by some routing protocols may not work in some environments.
- Many routing protocols may create redundant routes, which will greatly increase the routing updates as well as increase the whole networks overhead.

3.1. Energy Consumption of Wireless Ad-hoc Networks

Energy consumption is also one of the most important performance metrics for wireless ad hoc networks, it directly relates to the operational lifetime of the networks. Energy consumption is also one of the most important performance metrics because it directly relates to the operational lifetime of the network. Most research efforts are focused on performance comparisons and trade-off studies between various low energy routing and self-organization protocols, while keeping other system parameters fixed. As a result, very little has been revealed about the relationship between the aggregate energy consumption and non-protocol parameters such as node density and network coverage area.

IV. Security in Wireless Ad-hoc Networks

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. The system constraints include low-power, small memory and bandwidth, and low battery power. Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications. The main Ad-hoc Networks applications of MANET are in military and emergency, all these applications are security-sensitive. MENAT can not satisfy the security requirement of the applications of the architecture of MANET. There are several factors of security that we should consider. In this process maintain and develop of all military information secured in wireless ad-hoc networks.

4.1. Availability

First, Availability ensures the survivability of network services despite denial of service attacks. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable area.

4.2. Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

4.3. Integrity

Integrity guarantees that a message being transferred is never corrupted. A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

4.4. Authentication

Authentication enables a node to ensure the identity of the peer node. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

4.5. Non repudiation

Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

4.6. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

4.7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

4.8. Ordering

Out-of-order updates can also affect the correctness of the routing protocols. These messages may not reflect the true state of the network and may propagate false information. Ad hoc routing protocols have sequence numbers that are unique within the routing domain to keep updates in order.

4.9. Timeliness

Routing updates need to be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of the links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information. If a node that relays information between two large connected components is advertised as "down" by malicious neighbors, large parts of the network become unreachable. Most ad hoc routing protocols have timestamps and timeout mechanisms to guarantee the freshness of the routes they provide.

V. Security Aware Ad Hoc Routing (SAR)

We present a description of our protocol and its behavior and enumerate the metrics we deploy to measure the quality of ad hoc routing security of an ad hoc route discovered by our protocol. Finally & originally, ad hoc routing protocols were based on medications or augmentations to traditional routing protocols for wired networks [8]. These protocols send updates and react to topology changes, using monitoring and other infrastructure support to maintain routing tables. We study & developed the Current research focuses on pure on-demand [12, 17] routing protocols, and more recently, on augmentations that exploit additional information available on the ad-hoc nodes [26, 20, 21] to improve the quality of routes and reduce performance overheads. Most of the protocols that have been proposed so far focus on discovering the shortest path between two nodes as fast as possible. Some protocols trade performance and simplified management to obtain bounded sub-optimal paths to speed up the route discovery process [28, 16].

5.1. Protocol

Protocol is a set of rules created for the process of communication with another computer or with an operating system. In the original protocol, when a node wants to communicate with another node, it broadcasts a Route Request or RREQ packet to its neighbors. The RREQ is propagated to neighbors of neighbors and so on, using controlled flooding. The RREQ packets set up a reverse path to the source of the RREQ on intermediate routers that forward this packet. Moreover, SAR, we embed our security metric into the RREQ packet itself, and change the forwarding behavior of the protocol with respect to RREQs. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. SAR ensures that this node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level. Protocol maintain in rule regulation of Wireless Network.

5.2. Matrices of Protocol

We enumerate different techniques to measure or specify the quality of security of a route discovered by our generalized SAR protocol. The first technique is the explicit representation of trust levels using a simple hierarchy that reflects organizational privileges. SAR provides applications the ability to incorporate explicit trust levels into the route discovery process. Most organizations have an internal hierarchy of privileges. SRP defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information. The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes. For example, in our battlefield scenario, the military ranks of the users of the ad hoc nodes form an explicit partial-ordering of privilege levels. A simple way of incorporating trust levels into ad hoc networks is to mirror the organizational hierarchy, and associate a number with each privilege level. These numbers represent the security/importance/capability of the mobile nodes and also of the paths. Simple comparison operators can sort these levels to reflect their position in the actual hierarchy. We develop our notion of the "*level of protection*" associated with security of information in transit in routing protocol packets. Specifically, in SAR, the aim is to protect any information or behavior that can update or cause a change to the routing on cooperating nodes involved in an ad hoc routing protocol.

5.3. ARAN

A Secure Routing Protocol for Ad Hoc Networks (ARAN) [12] 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. Each node in ARAN receives a certificate after securely authenticating its identity to a trusted certificate server R. Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages. The certificate contains the node's IP address, its public key, as well as the time of issuing and expiration. These fields are concatenated and signed by the server R. A node P receives a certificate as: $R \rightarrow P : cert_P = [IP_P, L_P+, r, f] L_R-$. All the fields are concatenated and signed with source node I's private key. A combination of the nonce number (Q_I) and timestamp (r) is used to obtain data freshness and timeliness property. Source node I broadcasts a Route Discovery Packet (RDP) for a destination D as $I \rightarrow$ brdcst: $[RDP, IP_D, cert_I, Q_I , r]L_I-$. If G is the first node on the reverse path, REP packet is sent as $D \rightarrow G$: $[REP, IP_I, cert_D, Q_I, t] L_D-$. But nodes use an ERR message to report links in active routes broken due to node movement.

5.4. Cooperation of Nodes Fairness in Dynamic Ad-hoc NeT-works (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. 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.

5.5. Rushing attacks

Rushing attacks [9] 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.

5.6. 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.

5.6.1. 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.

5.6.2. Sybil Attack

In the Sybil attack [16], 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.

VI. Attack on Ad-hoc network and Secured Attacks using Modification

This attack disrupts the routing function by having the attacker illegally modifying the content of the messages. Examples of such attacks include redirection by changing the route sequence number and redirection with modified hop count that can trigger the black hole attack. Some other modification based attacks are presented next.

6.1. 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.

6.2. 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.

6.3. Blackmail Attack

Blackmail 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.

6.4. Resource Consumption Attack

In Fabrication attack part of resource consumption attack is 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.

6.5. Routing Table Poisoning

In Fabrication attack part of routing table poisoning is a malicious node sends false routing updates, resulting in sub-optimal routing, network congestion, or network partition.

6.6. Rushing Attack

In Fabrication attack part of rushing attack is malicious node in rushing attack attempts to tamper Route Request packets, modifying the node list, and hurrying its packet to the next node.

6.7. Black Hole

In Fabrication attack part of black hole is 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.

6.8. Masquerading

During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

6.9. 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.

6.10. 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 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.

6.11. Tunneling Attack

In a tunneling attack, two or more nodes collaborate and exchange en-capsulated messages along existing data routes. For example, if a Route Request 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.

VII. Security at the physical and data link layers and Solutions for Routing Protocols in Ad Hoc Wireless Networks

In this paper, we survey the security solutions in the mobile ad hoc networks. First we analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security

issues in the mobile ad hoc networks. We then point out various attack types that mainly threaten the mobile ad hoc networks. The Wireless Ad hoc Networks are a flawed architecture for the following solution technical reasons:

- The most important thing for the networks is security. It is even important for Wireless Ad hoc Networks because its applications are in military. The MANET cannot appropriately solve the problem of the security.
- Routing is also a big problem. All the routing protocols for Wireless Ad hoc Networks are need patches.
  In security at physical and data link layers are two types of faults that may occur in a routing algorithm: (i) faults whose effect is stochastically indistinguishable from ordinary link failures caused by the mobility of the system, radio interference, power failure etc, and (ii) faults whose effect can be distinguished from ordinary failures. Malicious faults tend to be of the second type, although the first type should not be excluded.

In this process of Message encryption and digital signatures are two important mechanisms for data integrity and user authentication. There are two types of data encryption mechanisms, symmetric and asymmetric (or public key) mechanisms. Symmetric cryptosystems use the same key (the secret key) for encryption and decryption of a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and another key (the private key) to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption purpose. Even if attacker comprises a public key, it is virtually impossible to deduce the private key. Any change to the message will produce a different hash result even when the same hash function is used. A MAC, which is a cryptographic checksum, is computed by the message initiator as a function of the secret key and the message being transmitted and it is appended to the message. The recipient re-computes the MAC in the similar fashion upon receiving the message.

7.1 Secure Efficient Ad hoc Distance Vector (SEAD)

Secure Efficient Ad hoc Distance Vector (SEAD) [7] is a proactive routing protocol, based on the design of DSDV [19]. 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. We collect all the nodes are creating, maintaining all the part of control ad-hoc secure process routing protocols update packets. 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.

SEAD provides a robust protocol against attackers trying to create incorrect 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.

7.2 ARIADNE

ARIADNE, 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. 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. 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 Route Error 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.

7.3. TIARA

Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) mechanisms protect ad hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on data traffic which are flow disruption and resource depletion.

7.4. Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP) [17], is another protocol extension 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. The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes. SRP assumes that this SA can be achieved through a shared key KST between the source S and target T. The source S initiates the route discovery by sending a route request packet to the destination T. The SRP uses an additional header called SRP header to the underlying routing protocol (e.g. AODV) packet. 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. 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. 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.

7.5. Defense Mechanisms against Wormhole Attacks

In order to prevent the wormhole attacks, the packet leashes mechanism [33] proposes to add additional information (referred as leashes) 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.

7.6. BISS

Building Secure Routing out of an Incomplete Set of Security Associations (BISS) [48], the sender and the receiver can establish a secure route, even if, prior to the route discovery, only the receiver has security associations established with all the nodes on the chosen route. Thus, the receiver will authenticate route nodes directly through security associations. The sender, however, will authenticate directly the nodes on the route with which it has security associations, and indirectly (by exchange of certificates) the node with which it does not have security associations. The operation of BISS ROUTE REQUEST relies on mechanisms similar to direct route authentication protocols. When an initiator sends a ROUTE REQUEST, it signs the request with its private key and includes its public key *PQR* in the request along with a certificate *sl* signed by the central authority binding its id with *PQR* .

VIII. Related Work

We develop our notion of the "level of protection" associated with security of information in transit in routing protocol packets. Specifically, in SAR, the aim is to protect any information or behavior that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. Attacks on the trust hierarchy can be broadly classified as Outsider Attacks and Insider Attacks, based on the trust value associated with the identity or the source of the attack. SAR modifies the behavior of route discovery, tying in protocol behavior with the trust level of a user. What is also needed is a binding between the identities of the user with the associated trust level. Routes discovered by SAR come with "*quality of protection*" guarantees. The techniques enabled by SAR can be easily incorporated into generic ad hoc routing protocols as illustrated by our implementation example - SAODV. In this chapter we discuss security services and challenges in an ad hoc wireless network environment. We research examine and classify major routing attacks and present a comprehensive survey on the state-of-the-art mechanisms and solutions designed to defeat such attacks. All routing protocol develops and executed from secured in this related process.

IX. Conclusions

We briefly introduce in this paper, the basic characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. SAR enables the discovery of secure routes in a mobile ad hoc environment. Its integrated security metrics allow applications to explicitly capture and enforce explicit cooperative trust relationships. In addition, SAR also provides customizable security to the flow of routing protocol messages themselves. In this paper, we examine security services and challenges in an ad hoc wireless network environment. We examine and classify major routing attacks and present a comprehensive survey on the state-of-the-art mechanisms and solutions designed to defeat such attacks. Finally we prove the current security solutions for the mobile ad hoc networks. In the end, we examine several security techniques that can help protect the mobile ad hoc networks from external and internal security threats. Even if parallel model checking approaches were used, our conclusion is that it is at this point not feasible to provide a proof for topologies of any significant size by modeling the protocol directly secured in ad-hoc wireless network.

X. Acknowledgements

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank Gauhati University, Assam (Teaching Staff of Department of Computer Science); S.B.M.S College, Sualkuchi, Assam; CMJ University for providing necessary facilities to carry out this work.

References

[1] J. Broch and D. B. Johnson. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks.IETF Internet Draft, October 1999.
[2] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Predistribution Scheme for Wireless Sensor Networks, ACM CCS 2003, Oct. 2003, pp. 42-51.
[3] 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.
[4] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
[5] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.
[6] Y. -C. Hu, D. B. Johnson, and A. Perrig, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, 2003.

[7] S.Chessa, P.Santi, "Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks", Proc. IEEE 20th Symp. on Reliable Distributed Systems (SRDS), New Orleans, pp. 257-266, October 2001.
[8] B. Leiner, R. Ruth, and A. R. Sastry, "Goals and challenges of the DARPA GloMo program," IEEE Personal Communications, vol. 3, no. 6, pp. 34–43, December 1996.
[9] A Distributed Light-Weight Authentication Model for Ad-hoc Networks.
[10] T. H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation, Proc. of IEEE Symp. On Wireless Personal Mobile Communications 2001, Sep. 2001.
[11] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. IEEE Network Magazine, November 1999.
[12] F. Wang, Brian Vetter, and Shyhtsun Felix Wu. Secure routing protocols: Theory and practice. Technical Report, North Carolina State University.
[13] B. Smith, S. Murthy, and J.J. Garcia-Luna-Aceves. Securing the Border Gateway Routing Protocols. In Global internet '96, London, UK, November 1996.
[14] C. E. Perkins and E. M. Royer. Ad-hoc On-Demand Distance Vector Routing. In The Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, February 1999.
[15] Jim Parker, Discussion Record for the 1st MANET Reading Group Meeting
[16] http://logos.cs.umbc.edu/wiki/eb/index.php/February_10%2C_2006 (Authorization required).
[17] Jiejun Kong, Xiaoyan Hong, Yunjung Yi, JoonSang Park, Jun Liu and Mario Gerlay, A Secure Ad-hoc Routing Approach Using Localized Self-healing Communities, in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 254–265, Urbana–Champaign, Illinois, 2005.
[18] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pages 275–283, Boston, Massachusetts, August 2000.
[19] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in Proceedings of ICNP'02, 2002.
[20] Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N., "Privacy vulnerabilities in encrypted HTTP streams" In Proc. Privacy Enhancing Technologies Workshop (PET 2005).
[21] J. Nam, S. Cho, S. Kim, and D. Won, "Simple and Efficient Group Key Agreement Based on Factoring" Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04), pp. 645-654, 2004.
[22] Panagiotis Papadimitratos , Zygmunt J. Haas, "Secure message transmission in mobile ad hoc networks, Ad Hoc Networks" IEEE 2003, 193–209 .
[23] Thomas S. Messerges, ohnas Cukier, Tom A.M. Kevenaar, Larry Puhl, Rene truik, Ed Callaway, "A Security Design for a General Purpose, Self-Organizing, Multihop Ad Hoc Wireless Network" 1st ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia 2003.
[24] Yih-chun hu, adrian perrig, "A Survey of Secure Wireless ad hoc routing" IEEE security & privacy May-June 2004.
[25] Ljubica Blazevic, Levente Buttyan, Srdan Capkun, Silvia Giordano, Jean-Pierre, Hubaux and Jean-Yves Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes".
[26] J. A. Freebersyser and B. Leinerr, "A DoD perspective on mobile ad hoc networks," in Ad Hoc Networking, C. E. Perkin, Ed. Addison-Wesley, 2001, pp. 29–51.
[27] B. Leiner, R. Ruth, and A. R. Sastry, "Goals and challenges of the DARPA GloMo program," IEEE Personal Communications, vol. 3, no. 6, pp. 34–43, December 1996.
[28] Perkins, C., Belding-Royer, E., Das, S.: Request for Comments: Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org/rfc/rfc3561.txt (2003).
[29] Johnson, D.B., Maltz, D.A., Hu, Y.C.: Internet draft: The dynamic source routing protocol for mobile ad hoc networks (DSR). http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt (2003).
[30] 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.