International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010
1793-8201

Taxonomy of Routing Security for Ad-Hoc Network

Rajendra Prasad Mahapatra, SM IACSIT and Mohit Katyal

***Abstract*—The emergence of the Mobile Ad Hoc Networking (MANET) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the proliferation of MANET-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in MANET, any node may compromise the routing protocol functionality by disrupting the route discovery process.**

***Index Terms*— Routing *Security, ARIADNE, DSR, MANET*.**

I. Introduction

The provision of security services in the *MANET* context faces a set of challenges specific to this new technology. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified in literature as such challenges. Nevertheless, the single most important feature that differentiates *MANET* is the absence of a fixed infrastructure. No part of the network is dedicated to support individually any specific network functionality, with routing (topology discovery, data forwarding) being the most prominent example. Additional examples of functions that cannot rely on a central service, and which are also of high relevance to this work, are naming services, certification authorities (*CA*), directory and other administrative services. Even if such services were assumed, their availability would not be guaranteed, either due to the dynamically changing topology that could easily result in a partitioned network, or due to congested links close to the node acting as a server. Furthermore, performance issues such as delay constraints on acquiring responses from the assumed infrastructure would pose an additional challenge.

The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them. In the *MANET* context, there may be no ground for an *a priori* classification, since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Additionally, in *MANET* freely roaming nodes form transient associations with their neighbors, join and leave *MANET* sub-domains independently and without notice. Thus it may be difficult in most cases to have a clear picture of the ad hoc network membership. Consequently, especially in the case of a large-size network, no form of established trust relationships among the majority of nodes could be assumed.

In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The mechanisms currently incorporated in *MANET* routing protocols cannot cope with disruptions due to malicious behavior. For example, any node could claim that is one hop away from the sought destination, causing all routes to the destination to pass through itself. Alternatively, a malicious node could corrupt any in-transit route request (reply) packet and cause data to be misrouted.

The widely accepted technique in the *MANET* context of route discovery based on broadcasting query packets is the basis of our protocol. More specifically, as query packets traverse the network, the relaying intermediate nodes append their identifier (e.g., *IP* address) in the query packet header. When one or more queries arrive at the sought destination, replies that contain the accumulated routes are returned to the querying node; the source then may use one or more of these routes to forward its data. Reliance on this basic route query broadcasting mechanism allows our proposed here *Secure Routing Protocol (SRP)* to be applied as an extension of a multitude of existing routing protocols. In particular, the *Dynamic Source Routing* (*DSR*) [1] and the *IERP* [2] of the *Zone Routing Protocol* (*ZRP*) [3] framework are two protocols that can be extended in a natural way to incorporate *SRP*. Furthermore, other protocols such as *ABR* [4] for example, could be combined with *SRP* with minimal modifications to achieve the security goals of the *SRP* protocol.

SRP guarantees the acquisition of *correct* topological information in a timely manner, i.e., the route replies that are validated and accepted by the querying node provide accurate connectivity information, despite the presence of

Manuscript received on September 9, 2009.
Rajendra Prasad Mahapatra is with SRM University as HOD (CSE) Mohit Katyal SRM University

strong adversaries. The protocol is proven robust against a set of attacks that attempt to compromise the route discovery, under the assumption of *non-colluding* adversarial nodes.

II. Security Services In Wireless Ad Hoc Network

In order to assure a reliable data transfer over the communication networks and to protect the system resources, a number of security services are required. Based on their objectives, the security services are classified in five categories [5]: availability, confidentiality, authentication, integrity and nonrepudiation.

•**Availability:** Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.

•**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.

•**Authenticity:** Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

•**Integrity:** Integrity guarantees that information passed on between nodes has not been tempered in the transmission. Data can be altered both intentionally and accidentally (for example through hardware glitches, or in case of ad hoc wireless connections through interference).

•**Non-repudiation:** Non-repudiation ensures that the information originator can not deny having sent the information. This service is useful for detection and isolation of compromised nodes in the network. Many authentication and secure routing algorithms implemented in ad hoc networks rely on trust-based concepts. The fact that a message can be attributed to a specific node helps making these algorithms more secure.

III. Security Mechanisms

Here we present security mechanisms specifically tailored for specific routing mechanisms.

A. Secure Efficient Ad Hoc Distance Vector (Sead)

Secure Efficient Ad hoc Distance Vector (SEAD) [6] is a proactive routing protocol, based on the design of DSDV [7]. 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 $0 < i \leq n$, 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, $0 < i \leq n$ 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 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

Can not 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.

B. *Ariadne*

ARIADNE [8], 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. However, for secure authentication of a routing message, it relies on the TESLA [9] broadcast authentication protocol.

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 (non-TESLA) 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 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.

ARIADNE provides a strong defense against attacks that modify and fabricate routing information. When it is used with an advanced version of TESLA called TIK, it is immune to wormhole attacks. However, it is still vulnerable to selfish node attack. General security mechanisms are very reliable but key exchanges are complicated, making ARIADNE infeasible in the current Adhoc environments.

C. Security Aware Routing (Sar)

Security Aware Routing (SAR) [10] is an on demand routing protocol based on 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 adhoc 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.

The initiator of the route in SAR includes a security metric in the route request. This security metric is the minimum trust level of the nodes that can participate in the route discovery. Consequently, only those nodes that have this minimum security level can participate in the route discovery. All other nodes that are below that trust level will drop the request packets. If an end-to-end path with the required security is found, the intermediate node or destination sends a suitably modified Route Reply. In the case of multiple paths satisfying the required security attributes, SAR selects the shortest such route. If route discovery fails, then a message can be sent to the initiator so that it can lower the trust level.

In the case of a successful path search, SAR always finds a route with quantifiable guarantee of security. This can be done by having nodes of a trust level share a key. Thus, a node that does not have a particular trust level will not possess the key for that level, and as a result it will not be able to decrypt the packets using the key of that level. Therefore, it will not have any other option but to drop the packet.

SAR uses sequence numbers and timestamps to stop replay attacks. Threats like interception and subversion can be prevented by trust level key authentication. Modification and fabrication attacks can be stopped by verifying the digital signatures of the transmitted packets.

One of the main drawbacks of using SAR is the excessive encrypting and decrypting required at each hop during the path discovery. In a mobile environment, the extra processing leads to an increased power consumption.

A route discovered by SAR may not be the shortest route in terms of hop-count, but it is secure. Such a path ensures that only the nodes having the required trust level will read and re-route the packets, but at the same time malicious node can steal the required key, a case in which the protocol is still open for all kinds of attacks.

D. Secure Routing Protocol (Srp)

Secure Routing Protocol (SRP) [11], 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. Such a security association should exist priori to the route initiation phase.

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. 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. 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.

E. Secure Routing Protocol For Ad Hoc Networks (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. Session keys are exchanged or distributed through a trusted third party like a certification authority.

Each node in ARAN receives a certificate after securely authenticating its identity to a trusted certificate server T. 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 T. A node A receives a certificate as: $T \rightarrow A : certA=[IPA, KA+, t, e] KT-$. In the authentication phase, ARAN ensures the existence of a

secure path to the destination. Each intermediate node in the network stores the route pair (previous node, the destination node). All the fields are concatenated and signed with source node I's private key. A combination of the nonce number (NI) and timestamp (t) is used to obtain data freshness and timeliness property. Each time I performs a route discovery, it monotonically increases the nonce. The signature prevents spoofing attacks that may alter the route or form loops. Source node I broadcasts a Route Discovery Packet (RDP) for a destination D as I → brdcst :[RDP, IPD, certI , NI ,t]KI−.Each node that receives the RDP for the first time removes any other intermediate node's signature, signs the RDP using its own key, and broadcasts it to all its neighboring nodes. This continues until destination node D eventually receives the packet.

After receiving the RDP, the destination node D sends a Reply (REP) packet back along the reverse path to the source node I. If J is the first node on the reverse path, REP packet is sent as D → J :[REP, IPI , certD, NI , t] KD−. When the source node I receives the REP packet, it verifies the destination's signature KD− and nonce NI . When there is no traffic on an existing route for some specific time, then that route is deactivated in the routing table. Nodes use an ERR message to report links in active routes broken due to node movement.

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.

F. Security Protocols For Sensor Network (Spins)

Security Protocols for Sensor Network (SPINS) [13] is a suite of two security building blocks which are optimized for ad hoc wireless networks. It provides important network services like data confidentiality, two party data authentication, and data freshness through Secure Network Encryption Protocol (SNEP) and secure broadcast through Micro Timed Efficient Stream Loss-tolerant Authentication (μTESLA).

Most of the current protocols are not practical for secure broadcast as they use asymmetric digital signatures. These signatures have high cost of creation and verification. SPINS introduces μTESLA 1), an enhanced version of TESLA which uses symmetric cryptographic techniques for authentications and asymmetry cryptography only for the delayed disclosure of keys. Tight lower bound on the key disclosure delay and robustness against DoS attacks makes μTESLA a very efficient and secure protocol for data broadcast.

SNEP provides point to point communication in the wireless network. It relies on a shared counter between a sender and a receiver in order to ensure semantic security. Thus it protects message contents of encrypted messages from eavesdroppers. Since both nodes share the counter and increment it after each block, the counter does not need to be sent with the message. In this way, the same message is encrypted differently each time. A receiver node is assured that the message originated from the legitimate node if the MAC verifies successfully. The counter value in the MAC eliminates replaying of old messages in the network.

SPINS is the first secure and lightweight broadcast authentication protocol. The computation costs of symmetric cryptography are low and the communication overhead of 8 bytes per message is almost negligible when compared to the size of a message. SNEP ensures semantic security, data authentication, replay protection, and message freshness whereas μTESLA provides authentication for secure data broadcast.

G. Cooperation Of Nodes Fairness In Dynamic Ad-Hoc Networks (Confidant)

Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) [14] 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.

Table 1: Summary of current security mechanisms

Protocol	*Security Mechanisms*	*Attacks Prevented*	*Comments*
SEAD [7]	- One-way hash chains	- Prevents an attacker from forging better metrics or sequence numbers in routing update packets	- Used with DSDV - Designed to protect routing update packets - Does not prevent an attacker from tampering other fields or from using the learned metric and sequence number for sending new routing updates
Ariadne [8]	- One-way hash chains	- Prevents attackers from tampering uncompromised routes consisting of uncompromised nodes - Immune to wormhole attack	- Used with DSR - Provides a strong defense against attacks that modify and fabricate routing information - Prone to selfish node attack
SAR [13]	- Quality of Protection (QoP) metric	- Uses sequence numbers and timestamps to stop replay attacks in routing update packets	- Used with AODV - Route discovered may not be the shortest route in terms of hop-count, but it is always secured - Defends gainst modification and fabrication attacks
SRP [17]	- Secure certificate server	- Defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information	- Used with DSR, ZRP - Lack of validation mechanism for route maintenance messages - Prone to wormhole attacks and invisible node attacks
ARAN [22]	- Secure certificate server	- Provides network services like authentication and non-repudiation	- Used with AODV, DSR - Heavy asymmetric cryptographic computation - Prone to wormhole attack if accurate time synchronozation is not available
CONFIDANT [2]	- Monitor - Reputation System - Path Manager - Trust Manager	- Attacks on packet forwarding and routing are defended efficiently	- Used with DSR - Detection based reputation system has few limitations - Vulnerable to spoofing and sybil attacks

IV. Conclusion

Achieving a secure routing protocol is an important task that is being challenged by the unique characteristics of an ad hoc wireless network. Traditional routing protocols fail to provide security, and rely on an implicit trust between communicating nodes.

In this paper we discuss 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. A summary of the secure routing mechanisms surveyed is presented in Table 1. The current security mechanisms, each defeats one or few routing attacks. Designing routing protocols resistant to multiple attacks remains a challenging task.

References

[1] D. B. Johnson et al, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, IETF MANET Working Group, March 2nd, 2001.

[2] Z.J. Haas, M. Perlman, P. Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," draft-ietf-manetzone ierp-01.txt, IETF MANET Working Group, June 1st, 2001.

[3] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of the Zone Routing Protocol" IEEE/ACM Transactions on Networking, vol. 9, no. 4, pp. 427-438, Aug. 2001.

[4] C.K. Toh, "Associativity-Based Routing for Ad-Hoc Mobile Networks, " Wireless Personal Communications, Vol. 4, No. 2, pp. 1-36, Mar. 1997.

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

[6] Y. -C. Hu, D. B. Johnson and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WM-CSA'02), Jun. 2002.

[7] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM'94 Conf. on Communications Architectures, Protocols and Applications, Aug. 1994, pp. 234-244.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, and A. Perrig, SPINS: Security Protocols for Sensor Networks, In Seventh Annual ACM Intl. Conf. on Mobile Computing and Networks (Mobicom 2001), 2001.

[14] 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.