SECURE REACTIVE ROUTING PROTOCOLS

Mr. Jitender Ahlawat
Assistant Proff.GITAM, Jhajjar(Haryana, India)

ABSTRACT

Mobile ad hoc networks (MANETs) are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Security is as important in ad hoc networks as it is in more traditional networks like the Internet. Security flaws of routing protocol may cause severe problems under ad hoc network. In this paper we briefly present the most popular on-demand routing protocol DSR and potential security problems of DSR. This paper analyzes security requirements for ad hoc routing protocols and review of the solutions provided for security problems such as ARIADNE, ARAN and CONFIDANT

Index Terms – MANET, Security, DSR

INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile nodes. Mobile Ad Hoc Networking (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. Providing adequate security measures for MANET is a challenging task.

The currently suggested routing protocols cope well with the dynamic topology, but usually offer little or no security measures. No single standard protocol captures common security threats and provides guidelines to make routing protocol secure

The Dynamic Source Routing protocol (DSR) was specifically designed for use in multi-hop wireless mobile ad hoc networks [1]. The DSR protocol does not require any existing network infrastructure or central administration and is completely self-organizing. DSR is a demand routing protocol, which means that no data is sent periodically and therefore it scales routing traffic and avoid the overhead package.

The following section presents background of securing the routing protocols. Section 3 presents a brief introduction to the ad hoc routing protocol DSR. Section 4 presents the possible attacks that a malicious node can use for disrupting the operation of a routing protocol in a self-organized

network and we analyze the already proposed secure ad hoc routing protocols that exist in the literature and present their operational principles.

LITERATURE REVIEW

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by Broch, Johnson, and Maltz [1].

In this section we will give a short overview of existing work and entry points to the literature. Zhou and Haas [2] primarily discuss key management. They devote a section to secure routing, but essentially conclude that "nodes can protect routing information in the same way they protect data traffic". They also observe that denial-of-service attacks against routing will be treated as damage and routed around.

Some work has been done by S. Marti, T. J. Giuli [3] to secure ad hoc networks by using misbehavior detection schemes. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving (especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures); and second, it has no real means to guarantee the integrity and authentication of the routing messages.

Kimaya Sanzgiri et al [4] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop), whereas the proposal presented in this paper only require originators to sign the message. In addition, it is prone to reply attacks using error messages unless the nodes have time synchronization.

Hubaux, et al. have proposed a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [5]. Kong, et al. [6] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the MAC address of multiple other nodes. Yi, et al. [7] also have proposed a general framework for secure ad hoc routing called the SAR.

Papadimitratos and Haas [8] proposed a protocol (SRP) that can be applied to several existing routing protocols. SRP requires that, for every route discovery, source and destination must have a security association between them.

Ariadne [9], by the same authors, is based on DSR [1] and TESLA [10] (on which it is based its authentication mechanism). It also requires clock synchronization.

S. Buchegger, and J.-Y. Le Boudec [11] proposed CONFIDANT routing protocol extension over DSR to provide security. In this paper we review secure routing protocols based on DSR.

DYNAMIC SOURCE ROUTING (DSR)

Routing protocols in mobile networks are subdivided into two basic classes:

• Proactive routing protocols

• Reactive routing protocols

The proactive routing protocols are table-driven. They usually use link-state routing algorithms flooding the link information. Link-state algorithms maintain a full or partial copy of the network topology and costs for all known links. The reactive routing protocols (e.g. DSR) create and maintain routes only if these are needed, on demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Thus, link-state routing algorithms are more reliable, less bandwidth-intensive, but also more complex and compute- and memory-intensive.

DSR reactive routing protocol works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link.

AD HOC NETWORK ROUTING SECURITY

The current proposed routing protocols for ad hoc wireless networks allow for many different types of attacks. Analogous exploits exist in wired networks, but are more easily defended against by infrastructure present in a wired network.

EXPLOIT ALLOWED BY DSR ROUTING PROTOCOL

DSR routing protocol has various vulnerabilities described below.

Attacks Using Modification : Malicious nodes can cause redirection of network traffic and DoS attacks by altering control message fields or by forwarding routing messages with falsified values. In modification DSR attacks through Denial-of-service with modified source routes and tunneling.

Attacks Using Impersonation : Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets, and is readily combined with modification attacks.

Attacks Using Fabrication : The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted. Falsifying routes and route cache poisoning attacks in DSR

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 in some cases incorporations of security mechanisms into existing ones (like DSR). As we will see, the design of these solutions focuses on providing countermeasures against specific attacks, or sets of attacks. The following routing protocols are extension to DSR to provide security.

(i) ARIADNE

Ariadne is a secure on-demand ad hoc routing protocol based on DSR proposed by Y. C. Hu, A. Perrig, and D. Johnson [9]. The security of Ariadne relies on the secrecy and authenticity of keys stored in nodes. Ariadne relies on the following keys to be set up, depending on which authentication mechanism is used:

- If **pairwise shared secret keys** are used, we assume a mechanism to set up the necessary n(n+1)/2 keys in a network with n nodes.
- If **TESLA** is used, we assume a mechanism to set up shared secret keys between communicating nodes, and to distribute one authentic public TESLA key for each node.
- If **digital signatures** are used, we assume a mechanism distribute one authentic public key for each node.

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. A node that generates a route error includes TESLA authentication details in the message. Therefore, every node that forwards the route error towards the destination of the message is able to authenticate it. The intermediate nodes buffer the route error message and its authentication does not take place until the node that generated it discloses the key.

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.

(ii) ARAN

ARAN was proposed by Sanzgiri et al in 2002 [4] , targeting to combat attacks including unauthorized participation, spoofed route signaling, alteration of routing messages, replay attacks, etc. Similar to other secure routing protocols, ARAN is also a security adds on over on-demand

routing protocols. It provides authentication, message integrity and non-repudiation as part of minimal security policy for ad hoc environment. ARAN is a security scheme, which can be applied to any on-demand routing protocols. It takes the advantages of PKI based digital signature scheme to provide security features including authentication, message integrity and non-repudiation.

ARAN consists of three stages: a preliminary certification process, a mandatory end-to-end authentication stage and an optional stage providing secure shortest path. To deploy these three stages, ARAN requires the use of a trusted certificate server *T* and public key cryptography. Each node, before entering the network, must request a certificate from *T*, and will receive exactly one certificate after securely authenticating their identities to *T*.

We provide a security analysis of ARAN by evaluating its robustness in the presence of the attacks introduced in Section 4. We also compare performance of ARAN to the DSR routing protocol [1].

Unauthorized participation: ARAN participants accept only packets that have been signed with a certified key issued by the trusted authority. In practice, many single-hop 802.11 deployments are already using VPN certificates; this is the case on the UMass campus. Mechanisms for authenticating users to a trusted certificate authority are numerous; a significant list is provided by Schneier. The trusted authority is also a single point of failure and attack, however, multiple redundant authorities may be used (e.g., as by Zhou and Haas [2]). Spoofed Route Signaling: Since only the source node can sign with its own private key, nodes cannot spoof other nodes in route instantiation. Similarly, reply packets include the destination node's certificate and signature, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or destination nodes are spoofed.

Fabricated Routing Messages: Messages can be fabricated only by nodes with certificates. In that case, ARAN does not prevent fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation. A node that continues to inject false messages into the network may be excluded from future route computation.

Alteration of Routing Messages: ARAN specifies that all fields of RDP and REP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be immediately detected by intermediary nodes along the path, and the altered packet would be subsequently discarded. Repeated instances of altering packets could cause other nodes to exclude the errant node from routing, though that possibility is not considered here. Thus, modification attacks are prevented.

Securing Shortest Paths: We believe there is no way to guarantee that one path is shorter than another in terms of hop count. Tunneling attacks are possible in ARAN as they are in any secure routing protocol. Securing a shortest path cannot be done by any means except by physical metrics such as a timestamp in routing messages. Accordingly, ARAN does not guarantee a shortest path, but offers a quickest path which is chosen by the RDP that reaches the destination first. Malicious nodes do have the opportunity in ARAN to lengthen the measured time of a path by delaying REPs as they propagate, in the worse case by dropping REPs, as well as delaying routing after path instantiation. Finally, malicious nodes using ARAN could also conspire to elongate all routes but one, forcing the source and destination to pick the unaltered route; clearly, a difficult task.

Replay Attacks: Replay attacks are prevented by including a nonce and a timestamp with routing messages.

(iii) CONFIDANT

CONFIDANT routing protocol was proposed by S. Buchegger, and J.-Y. Le Boudec [11], for making misbehavior unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Nodes cannot change their identifier to get rid of their reputation rating pre-defined lists of friendly nodes. CONFIDANT consists of the following components as: The Monitor, the Reputation System, the Path Manager, and the Trust Manager.

The monitor component of a CONFIDANT node is responsible for monitoring *passive acknowledgements* for each packet it forwards. When a node forwards a packet it monitors the transmissions of its next hop neighbors trying to detect deviations from the expected normal behavior. The trust manager component deals with the sending and receiving of *alarm* messages. These messages are generated and sent when the local node concludes that another node is misbehaving. Such messages are exchanged between nodes that are pre-defined as *friends*. Alarms from other nodes are given substantially less weight. The conclusion is reached based on the passive acknowledgements mechanism of the monitor component, or a received alarm message from another node. The reputation system component maintains a table of node identities and the associated ratings. Ratings are modified according to a *rate function* that uses small weights for reported alarms of malicious behavior and greater weights for direct observations. If a rating falls under a certain threshold the path manager component is called in order to remove the path containing the identified malicious node. Furthermore, the path manager ignores routing packets from the attacker and alerts (or ignores, this is a configuration setting) legitimate nodes when they request a route that uses a compromised path.

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.

Protocols	Attacks				
	Black hole	Replay	Worm hole	DoS	Routing table poisoning
ARIADNE	NO	YES	NO	YES	YES
ARAN	NO	YES	NO	NO	YES
CONFIDANT	YES	YES	NO	NO	NO

Defense against attacks

CONCLUSION

Existing routing protocols are subject to a variety of attacks. In this paper we review the security problems of DSR and routing protocols which provide security based on DSR. The main problem is to guarantee these security properties. Simulators can give excellent overview of protocol behavior but cannot ensure these properties. Therefore formal verification is needed, formal verification is a technique that assures a system has, or has not, a given property, based on a formal specification of the system under evaluation. We conclude that more work is needed towards a formal model based on solid mathematical grounds that can precisely give a definition for secure ad hoc routing. We decided to do the formal verification of AODV and DSR security properties and performance comparison of these two protocols through formal verification.

REFERENCES

[1] Dave B. Johnson and David A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, October 1999.

[2] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.

[4] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78-87.

[5] J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

[6] J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

[7] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.

[8] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[9] Y. C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Technical Report TR01-383, Rice University, Dec. 2001.

[10] A. Perrig, R. Canetti, D. Song, and D. Tygar. Efficient and secure source authentication for multicast. In *Network and Distributed System Security Symposium (NDSS'01)*, Feb. 2001.

[11] 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 Networking and Computing (MobiHoc 2002)*, ACM Press, 2002, pp. 226-236.