Ad Hoc On-demand Secure Source Routing

Roohie Naaz Mir and A M Wani
Department of Electronics & Comm. Engineering
National Institute of Technology, Srinagar,
Kashmir, 190006 INDIA

Abstract- **In mobile ad hoc networks, nodes do not rely on any routing infrastructure but the nodes route messages for each other. This communication set up functions properly only when the participating nodes co-operate with each other in routing and forwarding. It may, however, be advantageous for some nodes not to co-operate (e.g, to save power or get more bandwidth or to launch security attacks). This paper describes a routing protocol that is secure against attacks and uses some minimal trust levels amongst participating nodes. The set up uses source routing and no route caches are used. The idea is to route data on routes that are secure but may not be the shortest routes.**

I. INTRODUCTION

Wireless mobile ad hoc networks are a new paradigm of wireless communications proposed to support dynamic scenarios where no infrastructure exists. The lack of fixed infrastructure and the dynamic topology are the two main problems associated. The mobile hosts (nodes) that are within each others radio range communicate directly, while those that are far apart depend on other nodes to forward messages as routers. At the physical layer, the wireless channel suffers from signal interference, jamming, eavesdropping and distortion. These are taken care of by using spread spectrum, frequency hopping and error correcting codes. At the network layer most ad hoc routing protocols [4] are co-operative by nature and rely on trust relationships on their neighbors for routing packets among the participating nodes. The naïve trust model allows malicious nodes to paralyze an ad hoc network by inserting erroneous routing updates, replaying old routing information, changing routing updates or advertising incorrect routing information. These attacks are possible in fixed networks as well, but the ad hoc environment magnifies the attacks and makes detection difficult. Recently, a number of protocols have been proposed to secure the route discovery process in frequently changing ad hoc environments. The more widely used protocols in the ad hoc environment have been the reactive protocols where routes are discovered only when it is required by a node. For any protocol, it is assumed that all the participating nodes in a route would always relay without any misbehavior, which may not be realistic in a practical setting. The misbehavior may occur within the network or there may be an attack from outside. A routing protocol needs to be secure against or at least resilient against both the inside and the outside attacks.

In this paper, we present a secure ad hoc on-demand routing protocol that is robust against attacks. The protocol is based on source routing and starts by sending a route request (RREQ) to find a route to a destination. As a network is set up the neighboring nodes (1-hop only) exchange their public keys and IP addresses in order to set up a basic minimum trust level. As the route request arrives at a node, the node looks at the list of nodes with which it shares trust relationships and appends its IP address to the route request and the route request propagates through the network to the destination (D). As the route request arrives at the destination with IP addresses of all the intermediate nodes (IN) appended in the route, the destination calculates a Message Authentication Code (MAC). A route reply (RREP) packet is prepared and the MAC is appended to it and it is transmitted towards the source node (S) with the packet taking the same path as was taken by the route request. As the route reply arrives at S, a MAC is calculated and compared with the MAC in the header to validate the route reply. A number of route reply packets arrive at the S node but one with best metrics (minimum number of hops) is selected for transfer of data between the two nodes. The S node waits for the route reply packets in a predetermined time slot otherwise it sends a fresh route request packet.

As the route request and reply passes through nodes sharing some minimum trust level, it guarantees a distributed trust in the entire network. As nodes move and/or leave and join they again start by exchanging their public keys to establish their minimum trust levels. If any link breakage's are to be reported by IN's, the IN's need to sign the route error (RERR) packet. This helps in avoiding wrong reports from nodes. Any link breakage's or misbehaviors result in partitioning of the network and a route maintenance routine is invoked that starts a partial or complete route reconstruction depending upon the number of hops between the source and the broken link. This scheme uses minimum trust levels existing between nodes to find a secure route for data transfer without need for any link to link cryptographic validation that may be computationally costly for the battery operated and resource constrained nodes. The protocol gives preference to secure routes than faster routes. All breakage's or errors are to be reported to the S node and all decisions to start partial or complete reconstruction lies with the S node only.

The rest of the paper is organized as follows: Section II discusses the assumptions made for the protocol, section III discusses the related work, section IV discusses the proposed scheme:, comprising the route discovery and maintenance. Section V provides details about the simulations performed and the results thereof. Section VI provides the conclusions and section VII lists the references.

II. RELATED WORK

1-4244-0549-1/06/$20.00 ©2006 IEEE.

Most of the work on design of routing protocols in the on-demand side assumes all the participating nodes to be friendly nodes and there is not much published work regarding the security of the routing protocols. There are many works on securing the routing protocols in the fixed networks but the infra-structure-less have not been studied fully. Most of the mechanism in the fixed networks relies on a trusted third party or a server or a certification authority. In the un-tethered networks, nodes are mobile and they join and leave randomly, so none of the participating nodes can be entrusted with the job of performing key validation. Security is equally essential in this dynamic set-up but needs to be implemented from within the participating nodes and in a distributed manner.

Several researchers have recently studied the problem of secure and ad-hoc routing [1, 2, 3, 5, 6, and 8]. The mechanisms under study mainly fall into two categories, i.e., (i) prevention mechanisms, and (ii) detection and reaction mechanisms. Stajano and Anderson [1] elucidate some of the security issues facing ad-hoc networks and investigate ad-hoc networks composed of low compute-power nodes such as home appliances, sensor networks and PDA's where full public key cryptography may not be feasible. The authors develop a system in which wireless devices authenticate users by imprinting, and imprinting is realized by accepting a symmetric encryption key from the first device that sends such a key. They neither address routing nor forwarding. Zhou and Haas [2] proposed a secure routing protocol, which exploited threshold cryptography and relied on n-secret sharing servers to protect the routing information. If the bandwidth of the network is insufficient, the protocol may not be suitable. Papadimitratos and Haas [3] presented a secure routing protocol. The protocol relies on the secret association between the source and destination to protect the source routing messages. The novelty of the scheme is that false route replies, as a result of malicious node behavior, are discarded partially by benign nodes while in transit towards the querying node, or deemed invalid upon reception. The scheme disables route caching to avoid impersonation and relay attacks. However, there is no mention about any error messages. Marti and others [5] address the survivability of the routing service when nodes selectively drop packets. They take advantage of the wireless cards promiscuous mode and have trusted nodes monitoring their neighbors. Links with an unreliable history are avoided in order to achieve robustness. Although the idea of using promiscuous mode is interesting, the solution does not work well in multi-rate wireless networks because nodes might not hear their neighbors forwarding communication due to different modulations. In addition, this method is not robust against collaborating adversaries. Yi and others [6] study the security aware ad-hoc routing mainly with respect to some secure routing metrics and analyze AODV protocol with reference to these metrics and the work revolves round the authorization issues mainly. Perrig and others [8] propose protocols to study the devices that are severely constrained and where maximum security is to be extracted from the most minimal implementation possible. Our work in this paper also tries to arrive at a secure routing protocol with minimum trust levels existing amongst nodes in the network security and security is attained from a distributed setup. No route cache is being used. All routing decisions are made by the source node and minimum effort is expected by the IN's. Our work in this paper differs from the above in the assumption that nodes comprising the ad hoc network have a considerable computational power to perform some cryptographic functions.

III. Basic Assumptions

Any two nodes within the wireless communication range may interact with each other over the shared wireless channel. Each wireless interface may operate in promiscuous mode i.e. nodes A and B overhear each other's communications. A security association (SA) between the source node S and the destination D is assumed. The trust relationship could be instantiated, for example, by the knowledge of the public key of the other communicating party. The two nodes can negotiate a shared secret key K_{SD} (which would be assumed for the rest of the discussion) and using the security association (SA), verify that the principal that participated in the exchange was indeed the trusted node. The SA is bi-directional in that it can be used to control (data) traffic flow in both directions. The SA with any IN is unnecessary. Once the source and destination have established a secure route, they can further exchange a symmetric key and encrypt data packets to ensure confidentiality and integrity. All the nodes comprising the network are willing to participate in routing control and data packets. Nodes may move (in & out) at any time and without notice. Addressing in ad hoc networks is likely to follow recent trends towards dynamic address allocation and auto configuration. In these schemes, typically a node picks a tentative address and checks if it is already in use by broadcasting a query. If a conflict is found, the node is required to pick another tentative address and repeat the process.

In the ad hoc setting where nodes join and leave, and are allotted IP addresses dynamically, the key pairs that are shared between any two 1-hop neighbors are valid only till the node exists. As nodes move and are outside radio range, the public keys pertaining to that particular node are discarded and new keys are stored as new nodes arrive.

IV. Operation Of The Protocol

The protocol has two phases: route discovery and route maintenance. Route discovery phase starts by sending a RREQ packet when data is to be transferred between a source (S) destination (D) pair or a route previously being used has been broken and needs complete reconstruction. The maintenance phase is essential for reliable working of the protocol. The rest of the section describes the route discovery and route maintenance phases of the routing protocol in detail.

A. *Route Discovery*

This phase allows a node (source) to find the route to any other node (destination) dynamically, whether the nodes are in direct wireless range or not (by relaying through other nodes). The source node prepares a route request packet (RREQ) comprising of source IP address, destination IP address, a sequence number (for freshness) and broadcasts the packet. All nodes in the radio range receive it. Every

node compares the sequence number of this RREQ packet with any other RREQ packets received earlier from this node and if it has not been seen previously, it is stored for further processing otherwise it is discarded. The IP address of the source and the destination are stored in a table which also contains a count of all requests generated by this node in order to keep a count of the frequency of packets generated. The node next adds its IP address to the route and forwards it to all its 1-hop neighbors (to those sharing a secret key). The RREQ packet traverses towards the destination accumulating the route in the packet. As the RREQ packet arrives at the destination, a MAC is calculated over the route using the secret key shared between the source and destination. Hop count is also included in the MAC. The destination node prepares a route reply (RREP) packet and the calculated MAC is appended to it. The RREP contains the destination address, source address, number of hops, IP addresses of the intermediate nodes (forming the route) and the sequence number from the source node. The RREP takes a reverse path contained in the route and every intermediate node forwards it if and only if it had participated in finding the route to the destination. The intermediate nodes do not keep a record of the routes for other nodes and a particular route is valid only for a particular source destination pair. There is no route cache or a routing table that keeps details of any nodes. Instead every node has a small table that keeps record of messages sent to nodes and also (on account of promiscuous listening) messages relayed by nodes. This helps in detecting misbehavior. As the RREP arrives at the source node again a MAC is calculated and is compared with the one in the RREP packet. If they match, it is taken as a valid route reply, otherwise, it is discarded. One or more route replies arrive at the source and the one with the best metrics (minimum number of hops) is selected.

B. Route Maintenance

Conventional routing protocols include some periodic routing updates in the route maintenance procedure. In the on-demand routing no such updates are passed on, so some other technique is to be used like e.g., continuous monitoring by some node. We have a maintenance routine available that resides in every source node and this node becomes the sole authority for route maintenance (partial or complete) once a RRER message arrives at the node. Error messages can be reported by any of the nodes in the network but the messages are validated. The RERR packet contains the IP address of the node in error and its own IP address and a signature. This signature is sent to all 1-hop neighbors of the node for validation and RERR is taken as authentic only after this validation check. RERR packets may be due to link breakage's/communication faults or due to nodes moving away and not being within radio range or due to misbehavior like not relaying packets. The maintenance subroutine invoked depends upon the number of hops between the node reporting error and the source node. If number of hops between source and the broken node is more than half the hop count to the destination, a partial reconstruction is initiated otherwise a complete reconstruction is started.

V. Simulation And Results

The protocol has been simulated and tested using ns2 [12] simulator. Our work included detailed simulation of the proposed security solution in terms of number of neighbors, mobility, message overhead, tolerance to attackers, etc. Some of the features of the protocol like the number of RREP packets that can be received by the source before making a final choice was varied in order to find the effects on packet delay. An optimum number of RREP has to be fixed to get best possible results. Simulation results presented here include the following: (i) to find the average number of neighbors at a given value of mobility (fig. 1). This was done to find the number of nodes sufficient for relaying of packets; (ii) the average packet delay was observed in secure (keys exchanged) and in-secure (no keys exchanged) environments; (fig. 2) (iii) packets delivered for a fixed number of sources with varying mobility was observed; (fig. 3) (iv) varying amount of malicious activity was introduced in the network to observe the effect on number of packets delivered properly (fig. 4). Detailed analysis of the graphs and details about the data structures and frame formats used could not be included due to shortage of space.

VI. Conclusions

In this paper, we proposed a secure routing protocol for ad hoc networks that guarantees discovery of correct routes in presence of compromised or malicious nodes. The important features of the protocol are regulation of query propagation, acceptance of route error messages generated by nodes on the valid route and operation without an on-line certification authority. A node may use an arbitrary IP address while exchanging public keys, and every node's behavior in terms of packets generated (control and data) and transmissions received and forwarded is constantly under observation. Priority mechanism can be put into place in order to allow nodes generating minimum traffic to have better chance of using the network than those trying to throttle the network. Since the IN's do not have a possibility of sending any reply, therefore no node can advertise itself with a low value of hop count to allow the traffic to pass through itself. The simulation results have been compared with two other ongoing works on secure routing and the comparison study appears in a different communication.

VII. References

[1] F Stajano and R Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," *Proceedings of the 7th International Workshop on Security Protocols,* LNCS, pages 172-182. Springer Verlag.

[2] L Zou and Z J Haas, "Securing Ad Hoc Networks," *IEEE Networks,* 13(6): 24-30, Nov/Dec 1999.

[3] P Papadimitratos and Z J Haas, " Secure Routing for Mobile Ad Hoc Networks," *SCS Communications, Networking and Distributed Systems Modeling and Simulation Conference* (CNDS 2002) San Antonio, TX, January 27-31, 2002.

[4] E M Royer and C K Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications,* April 1999.

[5] S Marti, T Giuli, K Lai and M Baker, "Mitigating Routing misbehavior in Mobile Ad Hoc Networks," *In Sixth* Annual *ACM/IEEE International Conference on Mobile Computing and Networking,* Boston, MA, USA, Aug 2000.

[6] S Yi, P Naldurg and R Kravets, “Security-aware Ad Hoc Routing for Wireless Networks,” *In Proceedings of 2001 ACM International Symposium on Mobile Ad hoc Networking and Computing,* pages 299-302, ACM Press, 2001.

[7] D Balfanzo, D K Smetters, P Stewart and H C Wong, “Talking to Strangers: Authentication in Ad Hoc Wireless Networks," *In Proceedings of the ISOC 2002 Network and Distributed Systems Security Symposium,* Feb 2002.

[8] A Perrig, R Szewczyk, V Wen, D Culler and D Tygar, “SPINS: Security Protocols for Sensor Networks,” *Wireless Networks Journal (WINE),* Sep 2002.

[9] Chai Keong Toh, “A novel distributed routing protocol to support Ad hoc Mobile Computing,” *Proceedings of IEEE 15th Annual International Pheonix Conference on Computing and communication,* pp 480-486, March 1996,.

[10] D B Johnson and D A Maltz, “Dynamic Source Routing Protocol for Mobile Ad Hoc networks,” *Internet Draft, IETF, MANET Working Group,* Mar 2001.

[11] C E Perkins and E M Royer, “Ad Hoc On-Demand Distance Vector Routing,” Addison–Wesley, 2000.

[12] Network Simulator (ns2) available at http://www.isi.edu.

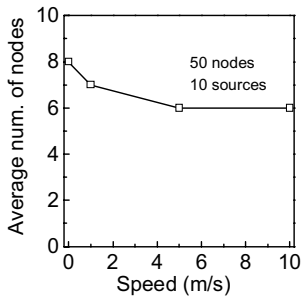

Fig. 1 Average number of neighbors

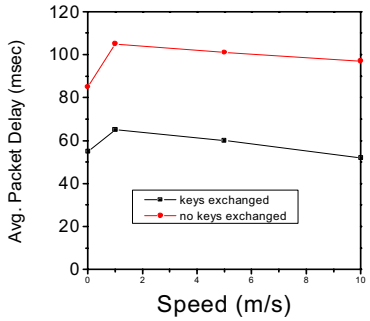

Fig.2 Avg. Packet delay with and without exchanging keys with 10 sources

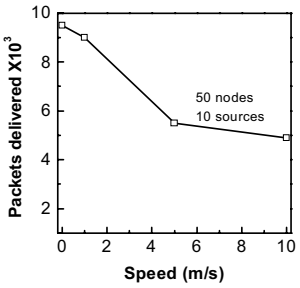

Fig.3 Number of Packets delivered (10 sources)

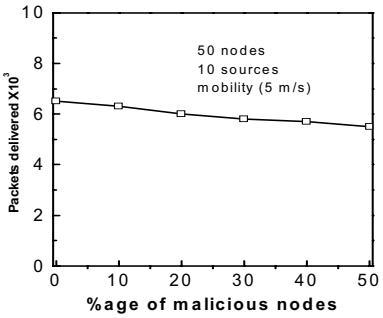

Fig.4 Number of Packets delivered