Secured On-Demand Multi-Path Routing in Trusted Environment based on Public Key Cryptography

R. Praveen Sam[1] Dr. P. Chandrasekhar Reddy[2] Dr. B. Stephen Charles[3]

ABSTRACT

An ad-hoc network is a collection of mobile nodes that establish and maintain connections purely over wireless connections. These networks do not have the infrastructure of a wired network. Because the nodes are mobile, links are continuously established and broken. An ad-hoc routing protocol must therefore provide for dynamic routing, where new paths can be created as soon as old paths become obsolete. The problem with many proposed routing protocols for ad- hoc networks is that these protocols have serious vulnerabilities to security attacks. Most recent ad-hoc network research has focused on providing routing services without considering major security issues. In this paper a new protocol is proposed to provide secure routing for ad-hoc networks that is based on public key cryptography. The proposed protocol is implemented using ASIM simulator.

Keywords : Mobile Ad-Hoc networks, Routing protocol, Security, Dynamic Source Routing, Cryptography.

1. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administration [1]. Such networks can be used to enable next generation of battlefield applications envisioned by the military [2], including situation awareness systems for managing war fighters, and remotely deployed unmanned micro-sensor networks. Ad- Hoc networks can also provide solutions for civilian applications such as disaster recovery and message exchanges among safety and security personnel involved in rescue missions. Several special properties lead to the uniqueness of MANET: Wireless media is used for communication, Network topologies and memberships are constantly changing, No predefined trust exists between communication partners, Limited bandwidth, battery lifetime, and computation power prohibits the deployment of complex routing protocols or encryption algorithms. While these characteristics are essential for the flexibility of a MANET, they introduce specific security concerns that are unknown or less severe in wired networks. Ad-hoc network routing protocols are challenging to design, and secure ones are even more so. A large number of routing protocols which cope well with the dynamic nature of ad hoc networks have been proposed[3,4,5,6,7,13,14,15].However, most of these routing protocols take security for granted and assume that every node in the environment is cooperative and trustworthy. Since these assumptions are not usually valid, a number of secure routing protocols for ad-hoc mobile networks have been proposed recently. Hence there is a need to design a new routing protocol to discover, evaluate and choose trusted routes based on multiple security metrics.

[1] Associate Professor , Dept of Computer Science and Engineering, Stanley Stephen College of Engineering , Kurnool – 518004, A.P, INDIA.
E-mail ; praveen_sam75@yahoo.com.

[2] Professor, Electronics and Communication Engineering, JNTU College of Engg, Hyderabad, A.P, INDIA.

[3] Principal, Stanley Stephen College of Engineering & Technology, Kurnool- 518004, A.P, INDIA.

The goal of this paper is to secure an already existing ad-hoc wireless network, DSR (Dynamic Source Routing) [7], by extending it in a way that non-malicious nodes can detect and isolate malicious nodes in the network so that they can not disrupt the network.

The rest of this paper is organized as follows. Section 2 describes about Routing Security issues. Section 3 discusses about new protocol, S_{DSR} (Secured DSR). Simulation results are presented in Section 4 and Section 5 concludes the paper.

2. Routing Security issues

To provide connectivity in a MANET, every host participates with other hosts to deliver packets to their destination. Since the communication safety of a host solely depends on a proper choice of the path used to reach the destination, it is important for a host to know the reliability of a route. The research problems in discovering trusted routes in wireless Ad Hoc networks are:

How to evaluate the trustworthiness of an individual host? A trust value is used to describe the ability of a host to forward packets or choose secure path.

How to evaluate the trustworthiness of a route through the trust value of the hosts along the path?

The research on trust and evidence formalization [8] provided insights to designing the trust model, propagating trust values among hosts, and assessing the trustworthiness of routes. When a host A chooses another host B to forward a packet, it takes some risk. Thus a trust relationship between A and B must be established. A degree of trust is used to estimate the risk and to help making rational decisions. A trusted route is a route that only involves trustworthy hosts. Sending packets through trusted routes will decrease the probability of malicious attacks and information leakage.

The following issues are considered in this research:

Issue 1: Applying trust metric to a single host, designing schemes to dynamically update the trust value, and assessing the trustworthiness of a route based on the involved hosts. The host's behaviors, such as forwarding, choosing proper routes, etc., are parameters that comprise the trust metrics. It is planned to investigate how to propagate trust from one host to another and how trust on hosts affects the trustworthiness of a route with respect to different forwarding schemes (e.g. source routing, hop-to-hop).

Issue 2: The design of an efficient trusted route discovery protocol for Ad -Hoc networks. The protocol must be scalable and adaptive, and can operate in on-demand or proactive fashion. The protocol will be capable of identifying trustworthy hosts by using authentication, and filtering erroneous query, and routing information. This routing protocol is an on-demand routing protocol for ad-hoc wireless networks in the sense that every node maintains routes only to the nodes that it communicates with. Furthermore, each node stores at most a predefined number of routes (namely, m) to each destination and for every packet will choose one of them randomly based on the trustworthiness of the nodes on the path. Using this strategy, we will avoid sending packets through previously trustworthy nodes that we believe might have been compromised. Although this goal is achieved at the expense of storing more route information at each node and multi-route discovery process (compared to on-demand protocols such as AODV [4] which require only one route), Section 5 shows that the amount of imposed extra overhead is reasonable in exchange for the achieved robustness.

3. About S_{DSR}

In this protocol, Public key cryptography [10] is used to protect the network against malicious nodes. Using encryption and public key signatures, the routing information is protected from being forged or tampered with. Before explaining the protocol operation, the assumptions and notations are provided those are followed in this protocol implementation. Assuming that, majority of nodes in network are trustworthy and only a small fraction are malicious. The connections in the network are bidirectional. Public and private keys of a node v are denoted by v_u and v_r respectively. Specifically, A_u and A_r represent public and private keys of the Certificate Authority (CA), which is a node that can issue/ revoke public key certificates to all other remaining nodes in the network [9]. Assuming that everybody knows the public key of CA. The stepwise explanation of our protocol is as follows:

Step 1: The first step and most difficult part of our protocol is establishment of trust environment between the mobile nodes. In this protocol, each node in the network must obtain a public key certificate from a trusted CA prior to joining the network. This certificate is a data structure which bounds IP of the new node with its public key. The CA issues certificates in an off-line process where each node proves its identity to the CA. Once issued, the certificates will not be revoked or expire during the lifetime of the network.

Step 2: The next step lies in the multi-path route discovery. Whenever a node s wants to communicate with another node d in the network, it should initiate a route discovery process if s is not aware of any paths to d or all such paths already known to s are broken. In order to initiate such a process, s signs and broadcasts a route request (RREQ) message: M= {RREQ, IP_d, T}, where T is a time stamp. Digital signature [9] is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Whenever an intermediate node v receives a route request message, it should simply sign and rebroadcast it. To protect RREQ message from malicious nodes, intermediate node verify each of the signatures in the RREQ message they received. If certificate of v appears somewhere in that sequence, the message should be discarded rather than be rebroadcast. This will prevent the RREQ message from being trapped in a loop. If an intermediate node receives the same route request message more than once from one of its neighbors, it should drop all but the first one. When the destination node d receives the first route request message from a source node s, it sets a timer for that node and starts to respond to every route request message it receives from s. Whenever d decides to reply to a route request, it should sign and send back a route reply message M= {RREP,IP_d,...,IP_s,T}, where T is a time stamp as before. Route reply messages are unicast back to s by the same intermediate nodes that broadcast the corresponding route request message. Again, each intermediate node verifies each of the signatures in the message. The intermediate node should sign the message and send it to the next hub on the path if all the tested signatures are valid. After t_{wait} seconds passed from receiving the first route request from s, or after m such requests were replied, d should drop and not reply to the same route request anymore.

Step 3: The next most important step is evaluation of trust of a node and a path. Trust is a value associated locally with a node. Trust of a path is sum of trust values of all nodes present in that path. For routing, the path with highest trust value is selected. In this protocol, every time a node d receives a packet from a node s via a path P,

it should send back an acknowledgement [12] for that packet using the same path. Every node s may know as many as m paths to another d. whenever s wants to send a message to d, it should decide which path to use based on their trust value. To do this, the node s has to keep track of all paths via which it has sent packets and whether or not it has received an acknowledgement for each packet. A path is chosen randomly by s. After a path is chosen, s appends a sequence number q_s and the chosen path to the data packet it wants to send, signs it and sends it via that path. Each intermediate node should simply forward such a packet, again verifying the signature of s. When node d receives a packet via a path $P=\{s,v_1,\ldots,v_n,d\}$, it should send back a signed acknowledgment $M=\{ACK,IP_{vn},\ldots IP_{v1},IP_s,q_s\}$ via the same path. Intermediate nodes forward this message back to s, again verifying the signature of d. Also the node s keeps a table of sequence numbers of packets it has sent, the path it has used and a time stamp for t_{ack} time units. Whenever it receives an acknowledgment, it increases trust values for each node present in that path. If after t_{ack}, s does not receive an acknowledgment, it punishes nodes in the corresponding path by decreasing their trust value. If an intermediate node v_k is unable to communicate with the next node while forwarding a data packet along a given route because of a network error, it should sign and send back a route error message $M=\{RERR, IP_{vk},\ldots,IP_{v1}, IP_s, q_s\}$ to s. Upon receipt of this message, s will locate and eliminate every path in its route cache which contains a link $\{IP_{vk}, IP_{vk+1}\}$.

4 Simulation Setup

The effect of S_{DSR} protocol was simulated using ASIM (Adhoc Simulator) simulator. It is the simulator that is developed for wireless ad-hoc network. Java has been chosen both for the implementation of the simulator itself and as the programming language of the simulated programs. This implies that the simulator is platform-independent and can be employed on all systems supporting the Java environment. Experiments were conducted with two sets, first without malicious nodes and the second with malicious nodes.

For the simulation, nodes were initially placed on a random location and a digital signature has been loaded to each node, which verifies the packet during communication process. A malicious node [11] is defined as a node that acts normally during the route discovering process, but drops all data packets, error and acknowledgement messages. In S_{DSR}, signature allows us to detect any kind of modification attacks and eventually modified packets are dropped with in the protocol.

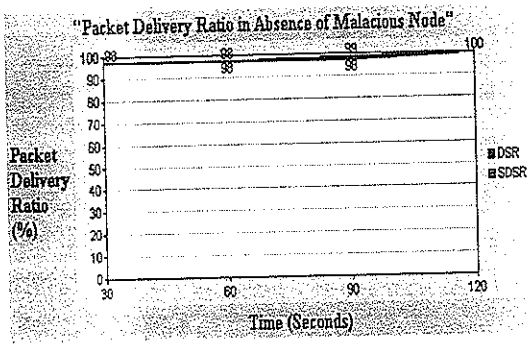
When a source node sends a route request to a destination node, a route table is created based on DSR Routing protocol. Following are the parameters used in the simulation.

Table 1. Simulation Parameter

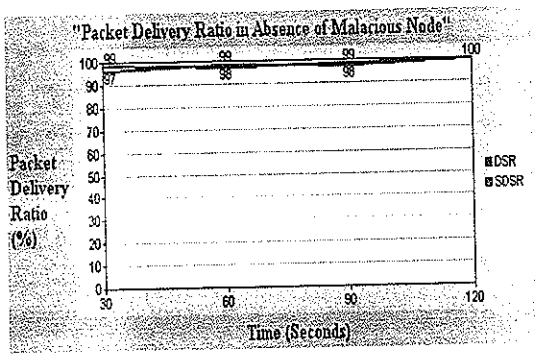
Parameter	Values
Number of Nodes	15, 20, 25, 30
Physical Terrain Dimensions	500m x 550m
Communication Range	175 m
Mobility	Static
Packet Size	120 bits
Trustworthy Threshold	1.0
Packet Delivery ACK Wait Time	2 sec
Maximum Speed	20m/s
Source Data Rate	4 packets/sec

There are several different metrics that can be applied to measure protocols performance against. Studies of performance evaluation of protocols for mobile ad hoc networks indicate that the throughput is the metric usually

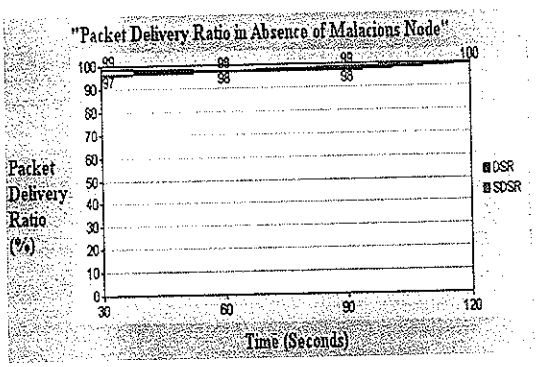
table, the packet delivery ratio is almost same for both protocols in absence of malicious nodes.



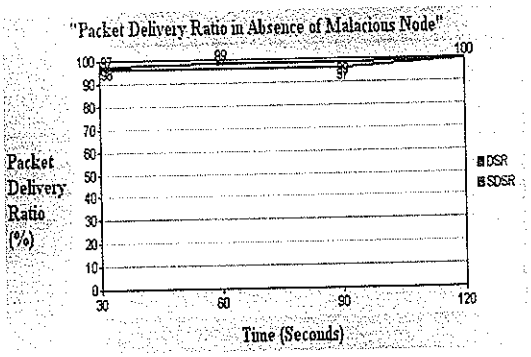
15 Nodes



20 Nodes



25 Nodes



30 Nodes

Figure 2. Packet delivery Ratio in the Presence of Malicious Nodes with the Network size of 15, 20, 25, 30 Nodes.

In the presence of malicious nodes, S_{DSR} outperforms over DSR as per our observation, Figure 2. The throughput is used to determine the influence of the trust based routing compared over standard DSR. Since DSR performs repetitive route testing in the presence of malicious nodes, its throughput decreases as number of malicious nodes increase in the network. But S_{DSR} discards the routes that have malicious node(s) so that route selection efficiency is improved, the communication delay is decreased and the throughput is increased.

We analyzed the performance of our protocol by increasing the number of nodes in the network and the number of malicious nodes as well. We compared the performance of our protocol with DSR, which implies that S_{DSR} performs well over DSR as the number of malicious nodes grows in the network.

In case of high mobility and higher number of route discovery operations, a large number of failure links also increase, resulting in more overhead over the communication. As per observation the throughput decreases as the number of malicious nodes in the network increases a certain amount. As seen, the throughput for DSR and route selection approach decrease when the number of malicious nodes moves towards 40%. The interval beyond 40 % malicious nodes is not examined because the results clearly indicate that the effect of trust based routing decreases beyond this point.

5. Conclusion

In this paper, a secured dynamic source routing protocol is presented. This protocol provides a solution for

securing on-demand multi-path routing in the trusted environment. Simulation results show that this protocol is as efficient as DSR in discovering and maintaining routes. In other words, this protocol is an extension of DSR to provide secure routing. As simulation results show that, this protocol give high throughput than DSR, even in the presence of upto 40% malicious nodes. Future work includes the ability of a node to authenticate another node in the network.

REFERENCES:

[1] M. Corson and A. Ephremides, "*A distributed routing algorithm for mobile radio networks*", MILCOM 89, 1989.

[2] R. Ramanujan and R. Edin. Tiara, *"Techniques for intrusion-resistant ad hoc routing algorithms"*, DARPA funded proposal, www.oracorp.com/projects/current/tiara.html, 2000-2003.

[3] C. Perkins and P. Bhagwat, *"Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers"*, *In ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, PP 234-244, 1994.

[4] C. Perkins and E. Royer, *"Ad-hoc-in-demand distance vector routing (AODV)"*, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, PP 90-100, 1999.

[5] Y.B. Ko and N.H. Vaidya, *"Location-aided routing (LAR) mobile ad hoc networks:*, In ACM/IEEE MOBICOM, 1998.

[6] V.D. Park and M.S. Corson. *"A highly adaptive distributed routing algorithm for mobile wireless networks"*, In INFOCOM (3), PP 1405-1413, 1997.

[7] D.B. Johnson and D.A. Maltz. *"Dynamic source routing in ad hoc wireless networks"*, In Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[8] B. Bhargava and Y. Zhong. *"Authorization based on evidence and trust"*. Data Warehouse and Knowledge Management Conference (DaWak), France, 2002.

[9] William Stallings, *"Cryptography and Network Security"*, 3rd edition, Pearson Education.

[10] N. Asokan and P. Ginzboorg. *"Key agreement in ad-hoc networks"*. Computer Communication Review, 23, PP 1627–1637, 2000.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, *"Mitigating routing misbehavior in mobile ad hoc networks"*, Proceedings of MOBICOM 2000, PP 255–265, 2000.

[12] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, *"Tcp selective acknowledgment options"*, 1996. RFC 2018.

[13] S. Yi, P. Naldurg, and R. Kravets, *"Security-aware ad-hoc routing for wireless networks"*, In MobiHOC Poster Session, 2001.

[14] L. Zhou and Z. Haas, *"Securing ad hoc networks"*, *IEEE* Network magazine, special issue on networking security, 13(6) pp 24–30, 1999.

[15] P. Papadimitratos and Z. Haas. *"Secure routing for mobile ad hoc networks"*. In *SCS* Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.

Author's Biography

R. Praveen Sam has completed B.Tech in Computer Science & Engineering from Sri Krishna Devaraya University, Anantapur and completed M.E from University of Madras, Chennai. Presently doing PhD from JNTU, Hyderabad. He has 5 years of teaching experience and published 1 International and 10 National conference papers. Presently he is working as Assoc. Professor in CSE Department, Stanley Stephen College of Engg & Technology, Kurnool, A.P.

Dr. P. Chandra Sekhar Reddy was born on 15-08-1966 at Chinnamanchupalle, Kadapa. He did his B.Tech (ECE) from JNTU, Anantapur in the year 1983, M.Tech Applied Electronics from Baratiar University. He did his Ph.D. from JNTU, Anantapur in the year 2001 on "Routing in Adhoc Networks". He worked as trainee at ISRO for 10 months. He has a total of 15 years of experience. Currently he is Professor ECE Department at JNTU, Hyderabad. He has published 4 papers in journals, 12 in conferences and he has also written 1 text book.

Dr. B. Stephen Charles has completed B.Tech in Electronics & Communication Engineering from Nagarjuna University, M.E from Bharathiyar University and PhD from JNTU, Hyderabad. He has 20 years of teaching experience and published 7 Journal papers, 20 International and 22 National conference papers. Presently he is working as Principal of Stanley Stephen College pf engg. & Technology, kurnool, A.P