A Encryption Based Dynamic and Secure Routing Protocol for Mobile Ad Hoc Network

Pankaj Kumar Sehgal pankajkumar.sehgal@gmail.com
Lecturer, MM Institute of Computer Technology and Business Management, MM University, Mullana (Ambala), Haryana, India

Rajender Nath rnath_2k3@rediffmail.com
Reader, Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India

ABSTRACT

Significant progress has been made for making mobile ad hoc networks secure and dynamic. The unique characteristics like infrastructure-free and absence of any centralized authority make these networks more vulnerable to security attacks. Due to the ever-increasing security threats, there is a need to develop algorithms and protocols for a secured ad hoc network infrastructure. This paper presents a secure routing protocol, called EDSR (Encrypted Dynamic Source Routing). EDSR prevents attackers or malicious nodes from tampering with communication process and also prevents a large number of types of Denial-of-Service attacks. In addition, EDSR is efficient, using only efficient symmetric cryptographic primitives. We have developed a new program in c++ for simulation setup.

Keywords: mobile network, ad hoc network, attacks, security threats

1. INTRODUCTION

While a number of routing protocols [9-17] have been proposed in the Internet Engineering Task Force's MANET working group in the last years, none of the address security issues satisfactorily. There are two main sources of threats to routing protocols. The first is from nodes that are not part of the network, and the second is from compromised nodes that are part of the network. While an attacker can inject incorrect routing information, reply old information, or cause excessive load to prevent proper routing protocol functioning in both cases, the latter case is more severe since detection of compromised nodes is more difficult. A solution suggested by [6] involves relying on discovery of multiple routes by routing protocols to get around the problem of failed routes. Another approach is the use of diversity coding [19] for talking advantage of multiple paths by transmitting sufficient redundant information for error detection and correction. While these approaches are potentially useful if the routing protocol is compromised, other work exists for augmenting the actual security of the routing protocol in ad hoc networks. The approach proposed in [25] complements Dynamic Source Routing (DSR, [17]), a popular ad hoc routing protocol, with a "watchdog" (Malicious behavior detector), and a "pathrater" (rating of network paths), for enabling nodes to avoid malicious nodes, the approach has the unfortunate side effect of rewarding them by reducing their traffic load and forwarding their messages. The approach in

[24] applies the concept of local "neighborhood watch" to identify malicious nodes, and propagate this information such that malicious nodes are penalized by all other nodes.

Efficient and reliable key management mechanisms are arguably the most important requirement for enforcing confidentiality, integrity, authentication, authorization and non-repudiation of messages in ad hoc networks, Confidentiality ensures that information is not disclosed to unauthorized entities. Integrity guarantees that a message between ad hoc nodes to ascertain the identity of the peer communicating node. Authorization establishes the ability of a node to consume exactly the resources allocated to it. Non-repudiation ensures that an originator of a message cannot deny having sent it. Traditional techniques of key management in wire-line networks use a public key infrastructure and assume the existence of a trusted and stable entity such as a certification authority (CA) [1-3] that provides the key management service. Public keys are kept confidential to individual nodes. The CA's public key is known to every node, while it signs certificates binding public keys to nodes. Such a centralized CA- based approach is not applicable to ad hoc networks since the CS is a single point of failure, which introduces the problem of maintaining synchronization across the multiple CAs, while alleviating the single-point-of-failure problem only slightly. Many key management schemes proposed for ad hoc networks use threshold cryptography [4-5] for distributing trust amongst nodes. In [6], n servers function as CAs, with tolerate at most t compromised servers. The public key of the service is known to all nodes, while the private key of the service is known to all nodes, while the private key is divided into n shares, one for each server. Each server also knows the public keys of all nodes. Share refreshing is used to achieve proactive security, and scalable adapt to network changes.

This proposal also uses DSR for illustration, describes DSR vulnerabilities stemming from malicious nodes, and techniques for detection of malicious nodes by neighboring nodes.

2. ENCRYPTED-DSR

EDSR has two phases: route discovery and route utilization phases. We give an overview of each phase below. A snapshot of the simulator for the same is shown in FIGURE 1.

2.1 Route Discovery

In the route discovery phase, a source node S broadcasts a route request indicating that it needs to find a path from S to a destination node D. When the route request packets arrive at the destination node D, D selects three valid paths, copy each path to a route reply packet, signs the packets and unicasts them to S using the respective reverse paths. S proceeds with the utilization phase when it receives the route reply packets.

2.2 Route Utilization

The source node S selects one of the routing paths it acquired during the routing discovery phase. The destination node D is required to send a RREP (Route Reply) packet to S. Then S sends data traffic to D.S assumes that there are selfish or malicious nodes on the path and proceeds as follows: S constructs and sends a forerunner packet to inform the nodes on the path that they should expect a specified amount of data from the source of the packet within a given time. When the forerunner packet reaches the destination, it sends an acknowledgment to S. If S do not receives an acknowledgment. If there are malicious agents in the path and they choose to drop the data packet or acknowledgment from D, such eventuality is dealt with cryptography so that malicious node can not get the right information.

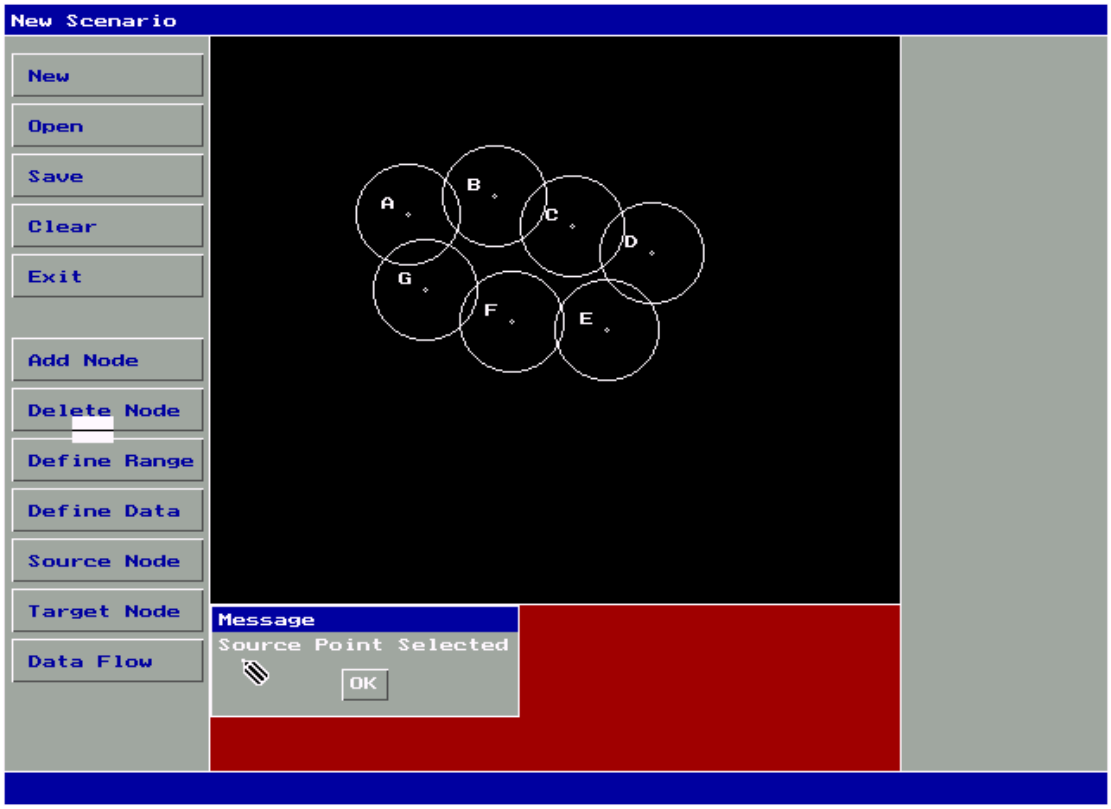


FIGURE 1: An ad hoc network environment for E-DSR

2.3 Network Assumptions

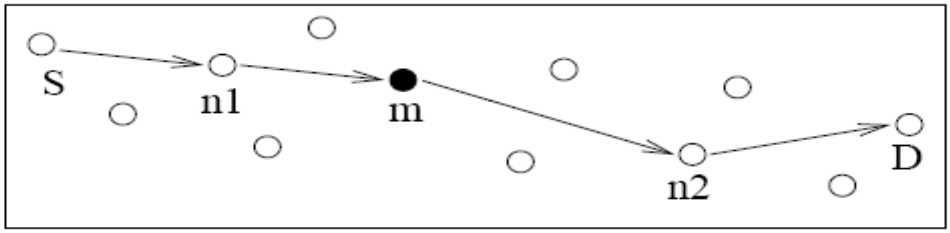
EDSR utilizes the following assumptions regarding the targeted MANETs:

- Each node has a unique identifier (IP address, MAC address).
- Each node has a valid certificate and the private keys of the CAs which issued the certificates of the other network peers.
- The wireless communication links between the nodes are symmetric; that is, if node Ni is in the transmission range of node Nj, then Nj is also in the transmission range of Ni. This is typically the case with most 802.11 [23] compliant network interfaces.
- The link-layer of the MANET nodes provides transmission error detection service. This is a common feature of most 802.11 wireless interfaces.
- Any given intermediate node on a path from a source to a destination may be malicious and therefore cannot be fully trusted. The source node only trusts a destination node, and visa versa, a destination node only trusts a source node.

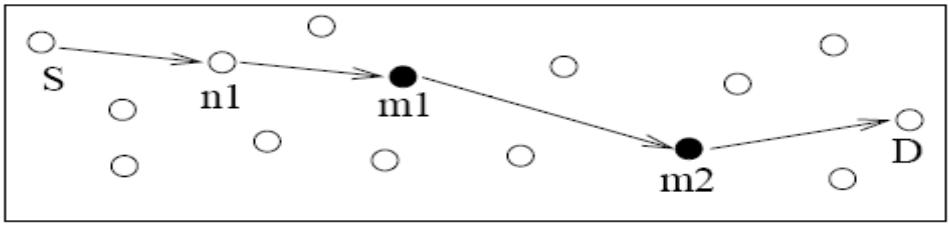
2.4 Threat Model

In this work, we do not assume the existence of security association between any pair of nodes. Some previous works, for example [7, 20] rely on the assumption that protocols such as the well known Diffie-Hellman key exchange protocol [18] can be used to establish secret shared keys on communicating peers. However, in an adversarial environment, malicious entities can easily disrupt these protocols - and prevent nodes from establishing shared keys with other nodes-by simply dropping the key exchange protocol messages, rather than forwarding them. Our threat model does not place any particular limitations on adversarial entities. Adversarial entities can intercept, modify or fabricate packets; create routing loops; selectively drop packets; artificially delay packets; or attempt denial of service attacks by injecting packets in the network with the goal of consuming network resources. Malicious entities can also collude with other malicious entities in attempts to hide their adversarial behaviors. The goal of our protocol is to detect selfish

or adversarial activities and mitigates against them. Examples for malicious nodes shown in FIGURE 2 and FIGURE 3.



FUGURE 2: One malicious node on a routing path



FUGURE 3: Adjacent colluding nodes on a routing path

2.5 Simulation Evaluation

We implemented EDSR in a network simulator using C language shown in Fig.5.1. For the cryptographic components, we utilized Cryptlib crypto toolkit [26] to generate 56-bit DES cryptographic keys for the signing and verification operations. In the simulation implementation, malicious nodes do not comply with the protocol. The simulation parameters are shown in TABLE 1.

Parameter	Value
Space	670m × 670m
Number of nodes	26
Mobility model	Random waypoint
Speed	20 m/s
Max number of connections	12
Packet size	512 bytes
Packet generation rate	4 packets/s
Simulation time	120 s

TABLE 1: Simulation Parameter Values

2.7 Performance Metrics

We used the following metrics to evaluate the performance of our scheme.

2.7.1 Packet Delivery Ratio

This is the fraction of data packets generated by CBR (Constant Bit Rate) sources that are delivered to the destinations. This evaluates the ability of EDSR to deliver data packets to their destinations in the presence of varying number of malicious agents which selectively drop packets they are required to forward.

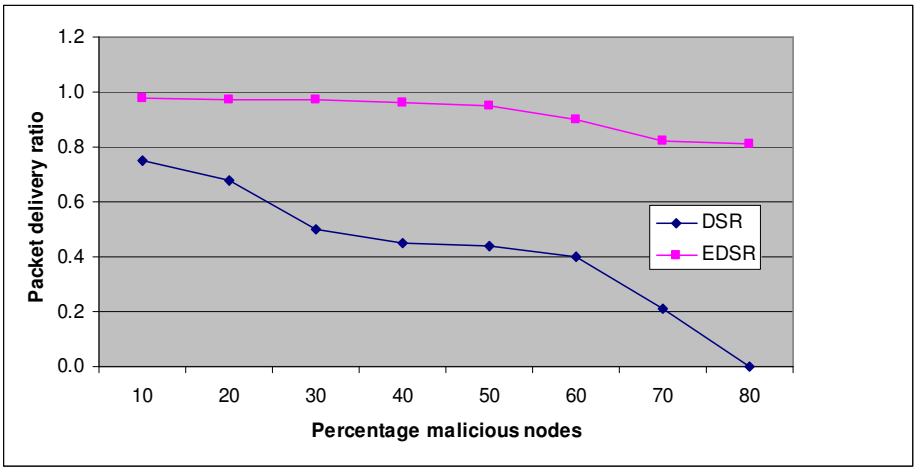


FIGURE 4: Data packet delivery ratio

2.7.2 Number of Data Packets Delivered

This metric gives additional insight regarding the effectiveness of the scheme in delivering packets to their destination in the presence of varying number of adversarial entities.

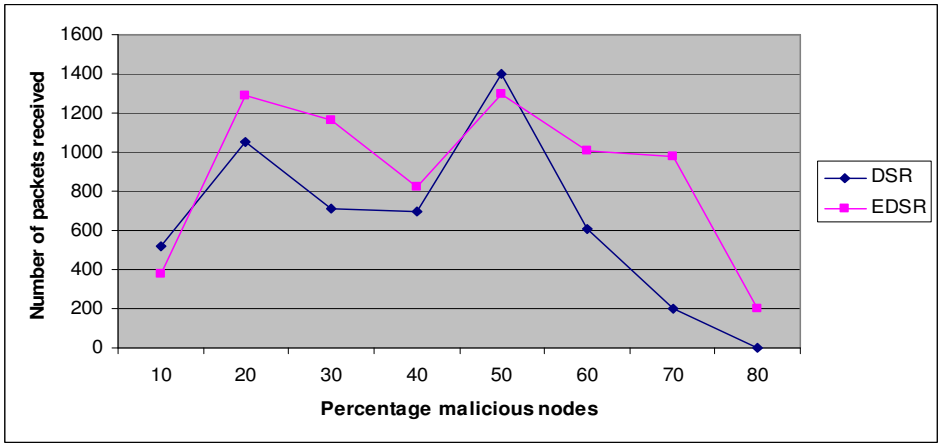


FIGURE 5: Number of packets received over the length of the simulation

2.7.3 Average End-to-end Latency of the Data Packets

This is the ratio of the total time it takes all packets to reach their respective destinations and the total number of packets received. This measures the average delays of all packets which were successfully transmitted.

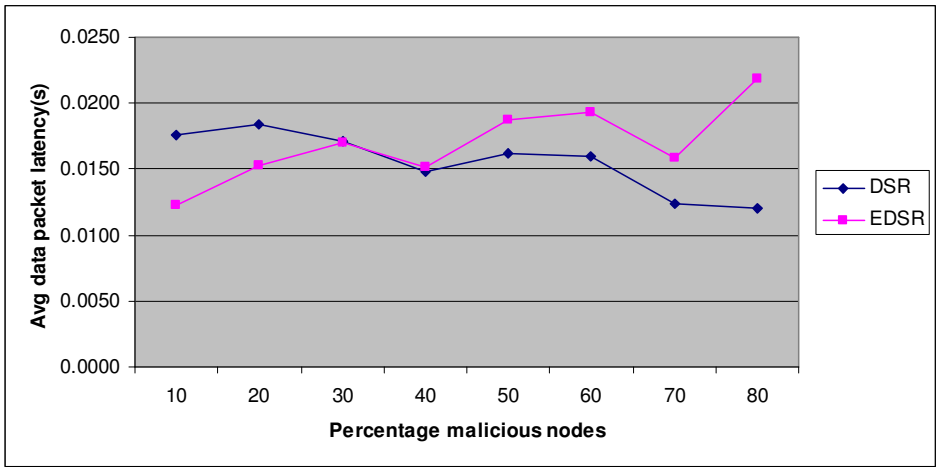


FIGURE 6: Average data packets latency

The results of the simulation for EDSR is compared to that of DSR [17], which currently is perhaps the most widely used MANET source routing protocol.

3. CONSLUSION & FUTURE WORK

Routing protocol security, Node configuration, Key management and Intrusion detection mechanisms are four areas that are candidates for standardization activity in the ad hoc networking environment. While significant research work exists in these areas, little or no attempt has been made to standardize mechanisms that would enable multi-vendor nodes to inter-operate on a large scale and permit commercial deployment of ad hoc networks. The standardization requirements for each of the identified areas will have to be determined. Based on the identified requirements, candidate proposals will need to be evaluated. Care has to be taken to avoid the trap that the MANET working group is currently in, which is of having of large number competing mechanisms. A protocol has been presented by us to standardized key management area. We have presented a simulation study which shows that E-DSR works better than DSR when malicious node increases.

In the future, complex simulations could be carried out which will included other routing protocols as well as other cryptography tools.

4. REFERENCES

1. M. Gasser et al., “The Digital Distributed Systems Security Architecture”, Proc. 12th Natl. Comp. Security Conf., NIST, 1989.
2. J. Tardo and K. Algappan, “SPK: Global Authentication Using Public Key Ceriticates”, Proc. IEEE Symp. Security and Privacy, CA, 1991.
3. C Kaufman, “DASS: Distributed Authentication Security Service”, RFC 1507, 1993.
4. Y. Desmedt and Y. Frankel, “Threshold Cryptosystems”, Advances in Cryptography- Crypto’ 89, G. Brassard, Ed. Springer- Verlag, 1990.
5. Y. Desmedt “Threshold Cryptography”, Euro. Trans. Telecom., 5(4), 1994.
6. L. Zhou and Z. Haas, “Securing Ad Hoc Networks”, IEEE Networks, 13(6), 1999.
7. 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 (WMCSA’02), Jun. 2002
8. C. S. R. Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: A Architectures and Protocols”, Prentice Hall PTR, 2004.

9. S. Das et Al. “Ad Hoc On-Demand Distance Vector (AODV) Routing”, draft-ietf-manet-aodv-17, February, 2003.
10. J. Macker et Al., “Simplified Multicast Forwarding for MANET”, draft-ietf-manet-smf-07, February 25, 2008.
11. I. Chakeres et. Al.,“Dynamic MANET On-demand (DYMO)Routing”,draft-ietf-manet-dymo-14, June 25, 2008.
12. I. Chakeres et. Al.,“IANA Allocations for MANET Protocols”,draft-ietf-manet-iana-07, November 18, 2007.
13. T. Clausen et. Al.,“The Optimized Link State Routing Protocol version 2”, draft-ietf-manet-olsrv2-06, June 6, 2008.
14. T. Clausen et. Al.,” Generalized MANET Packet/Message Format”, draft-ietf-manet-packetbb-13, June 24, 2008.
15. T. Clausen et Al., “Representing multi-value time in MANETs”, draft-ietf-manet-timetlv-04, November 16, 2007.
16. T. Clausen et Al., “MANET Neighborhood Discovery Protocol (NHDP)”, draft-ietf-manet-nhdp-06, March 10, 2008.
17. D. Johnson and D. Maltz., “Dynamic source routing in ad-hoc wireless networks routing protocols”, In Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996.
18. C. R. Davis., “IPSec: Securing VPNs”, Osborne/McGraw-Hill, New York, 2001.
19. E. Ayannoglu et al., “ Diversity Coding for Transparent Self-Healing and Fualt-Tolerant Communication Networks”, IEEE Trans. Comm. 41(11), 1993.
20. 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.
21. Y. Zhang and W.Lee, “Intrusion Detection in Wireless Ad Hoc Networks”, Proc. Mobicom. 2000.
22. R. Droms, “ Dynamic Host Configuration Protocol”, IETF RFC 2131, 1997.
23. IEEE-SA Standards Board. IEEE Std 802.11b-1999, 1999.
24. S. Buchegger and J. LeBoudec, “ Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustnes in Mobile Ad Hoc Network,” Proc. 10th Euromicro PDP , Gran Canaria, 2002.
25. S. Marti et al., “Mitigating Routing Behavior in Mobile Ad Hoc Networks”, Proc. Mobicom, 2000.
26. P. Gutmann. Cryptlib encryption tool kit. http://www.cs.auckland.ac.nz/~pgut001/cryptlib.
27 Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala, “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, in IJCSS: International Journal of Computer Science and Security, "Volume 2, Issue 3, pages 18-29, May/June 2008.
28. R.Asokan , A.M.Natarajan, C.Venkatesh, “Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad Hoc Networks”, in IJCSS: International Journal of Computer Science and Security, "Volume 2, Issue 3, pages 48-56, May/June 2008.
29. N.Bhalaji, A.Shanmugam, Druhin mukherjee, Nabamalika banerjee, “Direct trust estimated on demand protocol for secured routing in mobile Adhoc networks”, in IJCSS: International Journal of Computer Science and Security, "Volume 2, Issue 5, pages 6-12, September/ October 2008.