Proposed Protocol for Secured Multi Path Routing in Ad hoc Networks

Adnan Khurram
Department of Computers Science and Engineering

Abstract- Ad Hoc network is more convenient and cheaper than the networks with infrastructure in the usage and setup. As to wire network, the router and the terminals are also existed in Ad Hoc network. Compared with the roles of nodes in wire network, the major differences are which act two different roles meanwhile in Ad Hoc network. In practice, it is not only to research in communication security but also to setup the correct route becomes a very important subject. In this paper, I propose a new secure routing protocol based on IDMAC (Identity-Based Message Access code). According to my analysis, this scheme can prevent the problems of routing forging, modifying, and identity authentication on the Ad-Hoc network. Furthermore, I use NS2 (Network Simulator) to simulate our scheme and discuss how well the efficiency is from the simulation results.

I. INTRODUCTION

The common mobile network usually appears in forms, such as the cellular network or the wireless local area networks. Among cellular network, communication of portable terminal must finish with the aid of base station and switching of portable exchanger; in the wireless local area network, the portable terminal is connected to an existing infrastructural network through the wireless access point. However, today’s cellular networks use fix infrastructures, which are vulnerable to some special environments or the emergency such as the search and rescue after nature calamity. As a consequence, in such conditions, we need to rely on a kind of mobile communication network technology as the Ad Hoc network which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Furthermore, it requires no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed in the Ad Hoc network. They can be used in many special applications such as military usage, sensor networks, urgent and sudden occasion, and remote open-air area, interim occasions, personal communication, and business application. Until now, many routing protocols of Ad Hoc network are proposed [1], [2], [3], [4], [5], [6]. Compared with other traditional communication networks, there are several characteristics such as without a pre-existing infrastructure, dynamic topologies, dispose automatically, transmission bandwidth-constrained, and energy constrained operation in Ad Hoc network. Unfortunately, most of authors design originally routing protocols which mainly rely on the efficiency of the routing protocol and the quality of transmission of data. They do not consider the secure problem in the Ad Hoc network. Therefore, many experts and scholars have proposed different solutions to solve the secure problem in the Ad Hoc network [7], [8], [9], [10], [11]. According to our analysis, there are several difficult problems to reach the secure respect in these proposed Ad Hoc networks protocols. First, it is the key distribution problem between nodes. Generally, the authors have all supposed that the nodes already shared a common key each other or obtained others' public keys in advance. Secondly, in the Ad Hoc networks, the malicious node easily modifies the routing information or masks other nodes to forge routing information. How to protect the routing information and authenticate the identity is another difficult problem. In some papers, the authors do not particularly describe about their attack models, and not mention how much the influence degree is while the malicious nodes attack the network. Therefore, I need a secure scheme to solve these problems, and a completely attack scenarios analysis and simulation. I will propose a secure routing protocol for Ad Hoc network. Then, I will check this scheme whether it reaches our secure demand. At the same time, I will simulate two attack scenarios to this proposed scheme to verify the influence on Ad Hoc network.

II. ATTACKS TARGETING ROUTING PROTOCOLS

There are basically two types of security threats to a routing protocol, external and internal attackers [12]. An external attacker can be in the form of an adversary who injects erroneous information into the network and cause the routing to stop functioning properly. The internal attacker is a node that has been compromised, which might feed other nodes with incorrect information. Figure II.1 illustrates the different attacks that can be made towards a network [13].

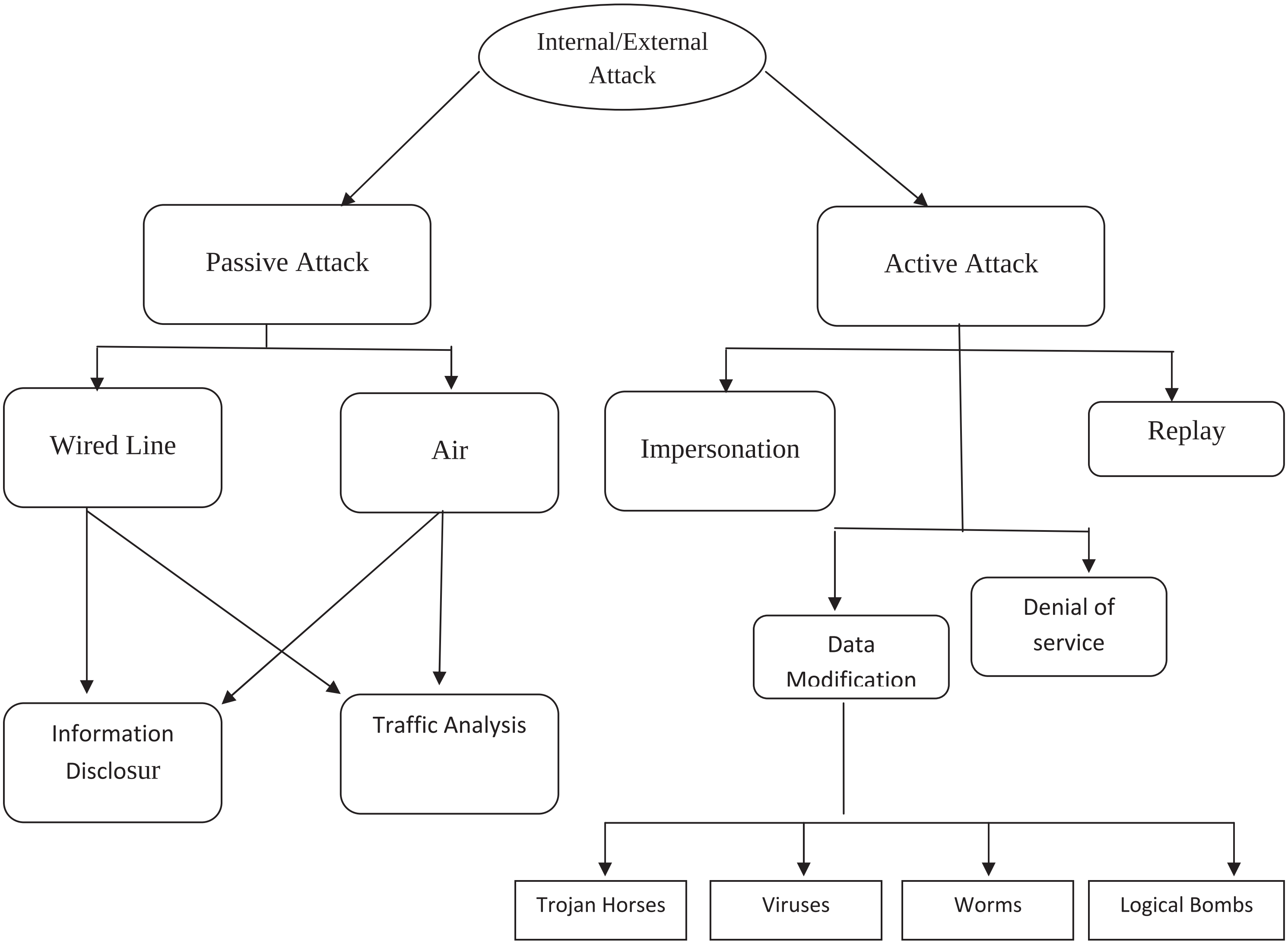

Figure II.1: Different sorts of attacks

A. Active and Passive Attacks

Security exposures of ad hoc routing protocols are due to two different types of attacks: active and passive attacks. In active attacks, the misbehaving node has to bear some energy costs in order to perform some harmful operation. In passive attacks, it is mainly about lack of cooperation with the purpose of energy saving. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

B. Malicious and Selfish Nodes in MANETs

Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network performances and eventually partition the network by simply not participating in the network operation [14]. In existing ad hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. Malicious nodes can easily perpetrate integrity attacks by simply altering protocol fields in order to subvert traffic, deny communication to legitimate nodes (denial of service) and compromise the integrity of routing computations in general. As a result the attacker can cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination increasing communication delays. A special case of integrity attacks is spoofing whereby a malicious node impersonates a legitimate node due to the lack of authentication in the current ad hoc routing protocols. The main result of spoofing attacks is the misrepresentation of the network topology that possibly causes network loops or partitioning. Lack of integrity and authentication in routing protocols can further be exploited through “fabrication” referring to the generation of bogus routing messages. Fabrication attacks cannot be detected without strong authentication means and can cause severe problems ranging from denial of service to route subversion. A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private connection bypassing the network. This exploit allows a node to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

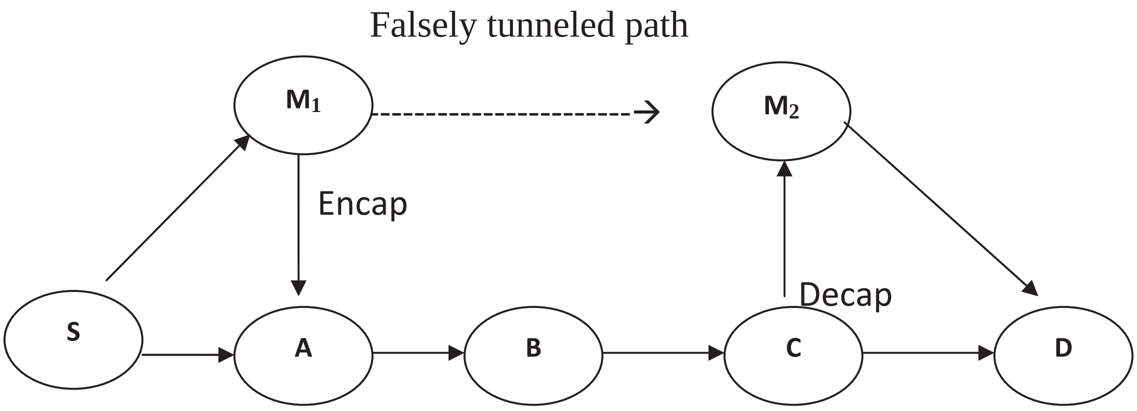

Figure II.2: Wormhole Attack

In the above figure, M1 and M2 are malicious nodes collaborating to misrepresent available path lengths by tunneling route request packets. Solid lines denote actual paths between nodes, the thin line denotes the tunnel, and the dotted line denotes the path that M1 and M2 falsely claim is between them. Let us say that node S wishes to form a route to D and initiates route discovery. When M1 receives a RDP from S, M1 encapsulates the RDP and tunnels it to M2 through an existing data route, in this case {M1->A->B->C->M2}. When M2 receives the encapsulated RDP, it forwards the RDP on to D as if it had only traveled {S->M1->M2->D}. Neither M1 nor M2 update the packet header to reflect that the RDP also traveled the path {A->B->C}. After route discovery, it appears to the destination that there are two routes from S of unequal length: {S->A->B->C->D} and {S- >M1->M2->D}. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 a better choice (in terms of path length) than the path to D via A. Another exposure of current ad hoc routing protocols is due to node selfishness that results in lack of cooperation among ad hoc nodes. A selfish node that wants to save battery life, CPU cycles and bandwidth for its own communication can endanger the correct network operation by simply not participating in the routing protocol or by not forwarding packets and dropping them whether control or data packets. This type of attack is called the black-hole attack. Current Ad Hoc routing protocols do not address the selfishness problem and assumes that all nodes in the MANET will cooperate to provide the required network functionalities**.**

III. PROPOSED PROTOCOLS SECURITY REQUIREMENTS

A. Routing Protocols Security Requirements–

To solve the security issue in an ad hoc network and make it secure we have to look at a number of requirements that have to be achieved. These requirements are: availability, confidentiality, integrity, authentication and non-repudiation [11].

- Availability: the network must at all times be available to send and receive messages despite if it is under attack. An attack can be in the form of a denial of service or an employed jamming to interfere with the communication. Other possible threats to the availability are if an attacker disrupts the routing protocol or some other high-level service and disconnects the network. The node itself can also be the problem to availability. This is if the node is selfish and will not provide its services for the benefit of other nodes in order to save its own resources like, battery power.
- Confidentiality: provides secrecy to sensitive material being sent over the network. This is especially important in a military scenario where strategic and tactical information is sent. If this information would fall into enemy hands it could have devastating ramifications.
- Integrity: ensures that messages being sent over the network are not corrupted. Possible attacks that would compromise the integrity are malicious attacks on the network or benign failures in the form of radio signal failures.
- Authentication: ensures the identity of the nodes in the network. If A is sending to B, A knows that it is B who is receiving the message. Also B knows that it is A who is sending the message. If the authentication is not working, it is possible for an outsider to masquerade a node and then be able to send and receive messages without anybody noticing it, thus gaining access to sensitive information.

Non-repudiation: makes it possible for a receiving node to identify another node as the origin of a message. The sender cannot deny having sent the message and are therefore responsible for its contents. It is particularly useful for detection of compromised nodes. However, because there are so many threats to protect from [15], there cannot be a general solution to them all. Also different applications will have different security requirements to take into consideration. As a result of this diversity, many different approaches have been made which focus on different parts of the problems. In the coming section, a comparison of some of the existing secure mobile ad hoc routing protocols with respect to most of the fundamental performance parameters will be given.

B. Authenticated Routing for Ad Hoc Networks Protocol (ARAN)

In this section, one of the secure mobile ad hoc networks (MANET) protocols, which are Authenticated routing for ad hoc networks (ARAN) is analyzed. Such protocol is classified as a secure reactive routing protocol, which is based on some type of query-reply dialog. That means ARAN does not attempt to continuously maintain the up-to-date topology of the network, but rather when there is a need, it invokes a function to find a route to the destination. In the following subsections, the details of the different phases of the ARAN secure routing protocol are presented. Furthermore, appendix B presents documentation for all the functions of ARAN secure mobile ad hoc network routing protocol.

I. Authenticated Routing for Ad Hoc Networks-

The ARAN secure routing protocol proposed by Sanzgiri, Laflamme, Dahill, Levine, Shields and Belding-Royer [16] uses cryptographic certificates to prevent and detect most of the security attacks that most of the ad hoc routing protocols face. This protocol introduces authentication, message integrity and non-repudiation as part of a minimal security policy for the ad hoc environment. ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. Thus, the routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination.

II. *Design Requirements-*

The following requirements are set while designing the reputation-based scheme to be integrated with the ARAN protocol:

a. The reputation information should be easy to use and the nodes should be able to ascertain the best available nodes for routing without requiring human intervention.
b. The system should not have a low performance cost because low routing efficiency can drastically affect the efficiency of the applications running on the ad hoc network.
c. Nodes should be able to punish other selfish nodes in the MANET by providing them with a bad reputation.
d. The system should be built so that there is an injection of motivation to encourage cooperation among nodes.
e. The collection and storage of nodes' reputation values are done in a decentralized way.
f. The system must succeed in increasing the average throughput of the mobile ad hoc network or at least maintain it.

IV.CONCLUSION

The field of MANETs is rapidly growing and changing. While there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years. One of these challenges is security. Security of mobile ad hoc networks has recently gained momentum in the research community. Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures [17] can be an impediment to basic network operation and countermeasures should be included in network functions from the early stages of their design. Security solutions for MANET have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure to rely on for building trust. To my knowledge, there is no previously published work on detecting and defending against malicious and authenticated selfish nodes together in the field of MANETs' routing protocols, even in the proposed secure routing protocols [18], [19], and [20]. Throughout , a discussion of existing mobile ad hoc networks' routing protocols' types and their advantages and disadvantages was given and a list of existing proactive, reactive and secure MANET routing protocols was compiled. Then, the different types of attacks targeting MANET routing protocols' security were explored. Also, the difference between malicious and selfish nodes and their associated attacks were discussed and a presentation of the fundamental requirements for the design of a secure routing protocol to defend against these security breaches was given. Furthermore, a comparison between some the existing secure mobile ad hoc routing protocols was presented. Then, an in-depth talk about the Authenticated Routing for Ad Hoc Networks protocol (ARAN) as one of the secure routing protocols built following the fundamental secure routing protocols design methodology was given. Afterwards, a discussion of how ARAN defends against most of the attacks that are conducted by malicious nodes such as spoofing, fabrication, modification and disclosure ones was presented. That resulted in proving that the currently existing specification of the ARAN secure routing MANET protocol does not defend against attacks performed by authenticated selfish nodes. Thus, I moved on discussing the different existing MANET cooperation enforcement schemes by stating their types: the virtual currency-based and the reputation-based schemes. Examples of each scheme and the different issues involved in the design of each were given. That resulted in proposing a new design of a reputation-based scheme to integrate it with one of the secure routing MANET protocols, ARAN, to make it detect and defend against selfish nodes and their misbehavior. In this proposal, the different phases of the proposed reputation-based scheme were explained. Then, an analysis of the various forms of selfish attacks that the proposed reputation-based scheme defends against was presented. Also, some time was invested in surveying the different simulation packages that are used in mobile ad hoc networks.

REFERENCES

[1] R. Hauser, A. Przygienda, and G. Tsudik, "Reducing the cost of security in link state routing", In Symposium on Network and Distributed Systems Security (NDSS '97), pages 93-99, San Diego, California, Feb. 1997. Internet Society.

[2] C. Parkins and E. Royer, "Ad Hoc on demand distance vector routing", 2^{m} IEEE workshop on mobile computing, pages 90100, 1999

[3] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication 800-48, November 2002.

[4] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining Digital Signatures and Public Key Cryptosystems", Communications of ACM, 21 (2), pp. 120-126, Feb. 1978.

[5] L. Lamport, "Password Authentication with Insecure Communication", Comm. of ACM, 24 (11), pp. 770-772, Nov. 1981.

[6] R. Perlman, "Fault-tolerant broadcast of routing information", In Computer Networks, u 7, pages 395-405, 1983.

[7] L. Zhou and Z. J. Haas, "Securing ad hoc networks", IEEE Network Magazine, 13(6):24-30, NovemberlDecember 1999.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the

[9] Sixth Annual International Conference on Mobile Computing and Networking, pages 255-265, 2000.

[10] B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UMCS-200l-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[11] Y. C. Hu, A Perrig and D. Johnson, "Ariadne: A secure ondemand routing protocol for ad hoc networks", Technical Report TROl-383, Rice University, Dec. 2001.

[12] Y. Hu, A. Perrig and D. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. Proceedings of second ACM Wireless Security, September 2003, pages 30-40.

[13] L. Zhou and Z. Haas. Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security. November/December 1999, pages 24-30.

[14] V. Gayraud and B. Tharon. Securing Wireless Ad Hoc Networks. ISS Master, MP 71 project, March 2003.

[15] P. Michiardi and R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. Proceedings of European Wireless Conference, February 2002.

[16] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, September 2002, pages 12-23.

[17] J. Hubaux, L. Buttyan and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. Proceedings of the second ACM Symposium on Mobile Ad Hoc Networking and Computing, October 2001, pages 146-155.

[18] K. Sanzgiri, B. Dahill, B. Levine, E. Royer and C. Shields. A Secure Routing Protocol for Ad hoc Networks. Proceedings of the tenth IEEE International Conference on Network Protocols, November 2002, pages 78-87.

[19] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, September 2002, pages 12-23.

[20] K. Sanzgiri, B. Dahill, B. Levine, E. Royer and C. Shields. A Secure Routing Protocol for Ad hoc Networks. Proceedings of the tenth IEEE International Conference on Network Protocols, November 2002, pages 78-87. P. Papadimitratos, Z. Haas and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. Internet-Draft, draft-papadimitratos-secure-routing-protocol-00.txt, December 2002.

[21] L. Zhou and Z. Haas. Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security. November/December 1999, pages 24-30.