An Analysis on Endaira:

A Provably Secure On-Demand Source Routing Protocol

A.F.A. Abidin, N.S.M. Usop
Faculty of Informatics
Universiti Darul Iman Malaysia, Kampus Kusza
21300 Kuala Terengganu, Terengganu
faisalamri@udm.edu.my, norsurayati@udm.edu.my

N.H.N. Zulkifli
Faculty of Computer Sciences and Information Technology
Universiti Malaysia Sarawak,
94300 Kota Samarahan, Sarawak
nznhuda@fit.unimas.my

***Abstract*—Routing is one of the most basic networking functions in mobile ad hoc networks. Secure routing protocols for mobile ad hoc networks provide the necessary functionality for proper network operation. Hence, an adversary can easily paralyze the operation of the network by attacking the routing protocol. This has been realized by many researchers, and several "secure" routing protocols have been proposed for ad hoc networks. There are some secure routing protocols that have been proposed to reduce the risk of attacking the routing protocol by Denial of Service, hackers and so on. In this research, we will explore and discuss a new on-demand source routing protocol, called ENDAIRA, and we demonstrate the usage of our framework by proving that it is most secure routing protocol. We assess the simulation study to compare and prove the strength of ENDAIRA model among the other secure routing protocol**.

***Keywords:* ENDAIRA, GlomoSim, MANET and Network Simulator 2**

I. INTRODUCTION

A mobile ad hoc network (MANET) is an infrastructure-less and autonomous network where a set of nodes are connected by wireless links where each node works as both a router and an end system. Due to the limited transmission range of wireless network interfaces, multiple nodes may be needed for one node to exchange data with another one across the network.

MANET routing protocols are vulnerable to attacks, such as denial of service, packet delay, packet modification, packet dropping, and spoofing. Both the ad hoc routing process and the data communication, or data forwarding, phases must be secured in order to provide a complete solution.

Routing has two main functions, which are route discovery and packet forwarding. The former is concerned with discovering routes between nodes, whereas the latter is about sending data packets through the previously discovered routes. There are different types of ad hoc routing protocols. OLSR protocol can distinguish as proactive while AODV and DSR protocols as reactive. Protocols of the latter category are also called on-demand protocols. AODV is another type of classification distinguishes routing table based protocols while DSR is a source routing protocols. In this paper, we focus on the route discovery part of on-demand source routing protocols. It is also show that the general principles of our approach are applicable to the route discovery part of other types of protocols.

At a very informal level, security of a routing protocol means that it can perform its functions even in the presence of an adversary whose objective is to prevent the correct functioning of the protocol. Since we are focusing on the route discovery part of on-demand source routing protocols, in our case, attacks are aiming at achieving that honest nodes receive "incorrect" routes as a result of the route discovery procedure.

Regarding the capabilities of the adversary, we assume that it can mount active attacks such as eavesdrop, modify, delete, insert, and replay messages. However, we make the realistic assumption that the adversary is not all powerful, by which we mean that it cannot eavesdrop, modify, or control all communications of the honest participants [1]. Instead, the adversary launches its attacks from a few adversarial nodes that have similar communication capabilities to the nodes of the honest participants in the network. This means that the adversary can receive only those messages that were transmitted by one of its neighbours, and its transmissions can be heard only by its neighbors. The adversarial nodes may be connected through proprietary, out-of-band channels and share information. We further assume that the adversary has compromised some identifiers, by which we mean that it has compromised the cryptographic keys that are used to authenticate those identifiers. Thus, the adversary can appear as an honest participant under any of these compromised identities.

The three properties must be maintained for a routing protocol to meet its objectives. A routing protocol is accurate

if it produces routes and reliable if it's returned routes are always accurate, even if non-malicious failures occur. In order to provide a security, a routing protocol needs to preserve the protocol's accuracy and reliability in the face of malicious attackers.

II. RELATED WORK

Many secure routing protocols have been recently proposed for MANET. These routing protocols aim to prevent the establishment of falsified routes. Security-Aware Ad hoc Routing (SAR) [2] is a general proposal that can be implemented with a reactive routing protocol. It defines the trust degree that should be associated with each node, and ensures that a node is prevented from handling a Route Request (RREQ) unless it provides the required level. This way, data packets will be sent only through trusted nodes, with respect to the defined level. Secure-AODV (SAODV) is an implementation of SAR on AODV. One of the difficulties of this approach is the definition of the trust level. Further, assuming that nodes showing the required trust level are genuine is not always correct.

Secure Routing Protocol (SRP) [3] is another secure routing protocol, based on Dynamic Source Routing (DSR). It prevents spoofing attacks, but it is vulnerable to the wormhole attack. We also find this vulnerability in Authenticated Routing for Ad hoc Networks (ARAN). ARIADNE is another DSR-based protocol that overcomes this attack. There are different implementations of this latter protocol. The first one is based on TESLA and the second uses Message Authentication Codes (MACs), and the most sophisticated uses digital signatures. However, it has been illustrated that this protocol is vulnerable to some fabrication attacks, which cause the construction of nonexistent routes. In order to mitigate this attack, ENDAIRA [2] has been proposed, which is very similar to the last version of ARIADNE. Its idea is simply to sign Route Reply (RREP) packets instead of RREQ. Note that all these secure routing protocols do not handle packet dropping misbehaviour, hence they are vulnerable to the black hole attack, and to the selfish behavior.

While their goal is to find a route between a source and destination, these protocols do not contain mechanisms to prevent malicious route manipulation. There are numerous proposed secure routing protocols intended to guard against corrupt routes and ensure malicious outsiders are not included in discovered routes. Solutions intended to secure the routing process include the Source Routing Protocol (SRP), ARIADNE, Security-Aware ad hoc Routing (SAR), Secure Efficient Ad hoc Distance Vector (SEAD), Secure AODV (SAODV), Authenticated Routing for Ad hoc Networks (ARAN), Secure Position Aided Ad hoc Routing (SPAAR), and the Secure Link State Routing (SLSR) protocols.

In MANETs each node acts as a router forwarding data to other nodes. Once routes are established via secure route discovery, two phased routing protocols continue to be vulnerable to attacks against the data forwarding phase. Malicious insiders, or Byzantine attackers, are legitimate routing entities, since malicious insiders are fully trusted and hold certified cryptographic keys. It is impossible to identify a corrupt insider until the node acts maliciously. As long as a malicious node forwards data according to protocol rules, it is not a threat since the data successfully reaches its destination. Once malicious activity occurs, secure ad hoc routing protocols must take steps to mitigate the effects. Mitigation strategies may include utilizing multi-path routing protocols or using protocols that identify and eliminate malicious nodes from route caches or future route discovery.

Another mitigation strategy for attacks against the data forwarding phase is to monitor links for malicious activity and eliminate or avoid nodes exhibiting malicious behavior. Methods utilizing this approach include the *watchdog-pathrater*, On-Demand Secure Byzantine Routing (ODSBR), CORE, and CONFIDANT protocols. Additional concepts proposed to protect against misbehaving nodes include random two-hop acknowledgments, *iterative* and *unambiguous* probing mechanisms, and signed tokens.

III. PROBLEM OVERVIEW

In [1] and [3], previous secure routing protocol proposed is ARIADNE and it has been proposed as a secure on-demand source routing protocol for ad hoc network. In ARIADNE, there are some attacks to this protocol and it makes ARIADNE is not considering as the most secure routing protocol. Let illustrate the problem as figure 1 below where A needs to send data to B through the network. The major issue is to make sure the data is secure and arrives safely without any attacks from the adversary. Let assume that adversary on Z nodes.

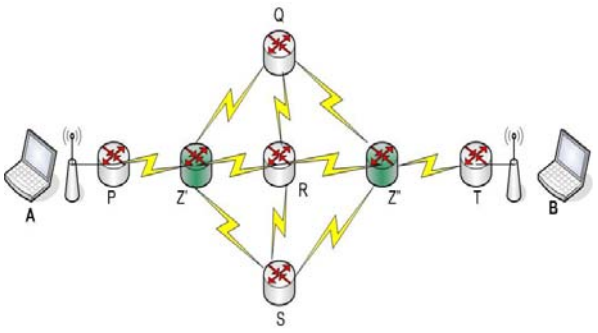

Figure 1. An adversary control 2 nodes Z' and Z" in the topology

An adversary can easily paralyze the operation of the network by attacking the routing protocol. However, the security of those protocols has been analyzed either by informal means only, or with formal methods that have never been intended for the analysis of this kind of protocols, for instance, BAN logic. In other words, the adversary is able to divert the communication between *A* and *B* through itself, and then control the data.

One more issues is when dealing with the selfish misbehavior or the packet dropping attack [2], most of the solutions are more focus on data packets and not directly applicable to control packets. The number of control packets is too low compared with the data packet. Nonetheless, dropping control packets may be beneficial for selfish nodes and malicious ones as well.

For example, by dropping the RREQ packets a selfish node could exclude itself from routes and thereby avoid receiving data packet to forward. A malicious could drop Route Error (RERR) packets to keep the use of failed routes, potentially resulting in a denial of service.

IV. ENDAIRA: A SECURE ON-DEMAND SOURCE ROUTING PROTOCOL

A. *Modelling ENDAIRA*

The ENDAIRA protocol [3] attempts to secure DSR by securing only the return *rrep* using cryptographic signatures. The ENDAIRA forward *rreq* is identical to DSR, using no cryptographic mechanisms to secure the *rreq*. This approach is different than SRP's attempt to secure the forward *rreq* process and ARIADNE's attempt to secure both the forward *rreq* and return *rrep* processes.

The ENDAIRA message formats follow as:

1) <*rreq*, initiator, target, id, accum_path>
2) <*rrep*, initiator, target, accum_path, sig_list>

We illustrate the ENDAIRA protocol using the network topology and message sequence shown in figure 2 and 3.

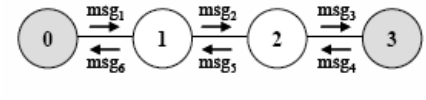

Figure 2. ENDAIRA network topology

msg_1 = (rreq, 0, 3, id, ( ))
msg_2 = (rreq, 0, 3, id, (1))
msg_3 = (rreq, 0, 3, id, (1, 2))
msg_4 = (rrep, 0, 3, (1, 2), (sig_3))
$sig_3 = SK_3${rrep, 0, 3, id, (1, 2), ()}
msg_5 = (rrep, 0, 3, (1, 2), (sig_3, sig_2))
$sig_2 = SK_2${rrep, 0, 3, (1, 2), (sig_3)}
msg_6 = (rrep, 0, 3, (1, 2), (sig_3, sig_2, sig_1))
$sig_1 = SK_1${rrep, 0, 3, (1, 2), (sig_3, sig_2)}

Figure 3.ENDAIRA message sequence

Node 0 is the initiator, node 3 is the target, and *SKi* is node *i's* signing key. Instead of protecting the forward *rreq* process, the target computes a signature over the accumulated path received in the *rreq* and adds the signature to the *rrep*. During the *rrep*, the intermediate nodes sign the message and forward to the next hop. Once the *rrep* reaches the initiator, the initiator checks the target signature and verifies that each node in the return path has signed the message in reverse order. While the target may sign corrupted paths received by the *rreq*, the protocol authors contend that false paths should not be successfully returned to the initiator with the correct appended signatures.

We validate the ENDAIRA model to ensure that the paths are correctly constructed, the target signature protects the reverse *rrep*, and the intermediate node signatures are appended in the proper order during the *rrep* and compared against the signed accumulated path.

V. SIMULATION ASSESSMENT

Previous research used GlomoSim simulation to run the experiment [2]. For this research, we used Network Simulator 2 (NS-2) as the simulations tools and we will compare the results which produced by these two simulation tools. There are 5 nodes that being used as a simulation model. The nodes are node 0, node 1, node 2, node 3 and node 4. Assume that node 4 has been controlled by an adversary.

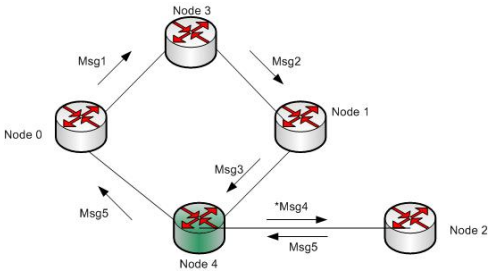

Figure 5. Simulation Model

We simulated a network of 50 nodes, moving in an area of $1500x1000m^2$ according to the random-waypoint model, during 30 minutes. Each node has a power range of $250m$. We change the nodes' speed from $0m=s$ to $4m=s$, and for each value of the mobility we made the measurements for three different configurations of misbehaving:

1) Low misbehaving rate with 5 misbehaving nodes.
2) Medium rate with 12 misbehaving nodes.
3) High rate in which 20 nodes misbehave.

For each configuration we used 5 seeds, resulting in no less than 2000 scenarios. The curves presented hereafter represent the averaged values for those configurations. Performance metrics that being used in this paper are True Isolation Rate, False Isolation Rate and End to End Delay which occurred in the experiment.

VI. Results and Analysis

As in [2], this experiment simulated two kinds of packet dropping. RREQ dropping, which represents the selfish misbehavior and allows evaluating our solution for broadcast packets, and RERR dropping that represents a malicious behavior aiming a DoS attack, which allows evaluating the solution with respect to broadcast packets.

A. Phase 1: Results and Analysis

We set the phase 1 experiment, and compare our basic ENDAIRA with NS-2 and basic ENDAIRA with GlomoSim. For the comparison, we used the GlomoSim results as in the previous results [2]. Referring to our results, figure 6.0 shows how our protocol, has high true isolations, especially when the mobility increase. ENDAIRA with NS-2 shows some changes in the previous results but we found that the pattern is almost the same.

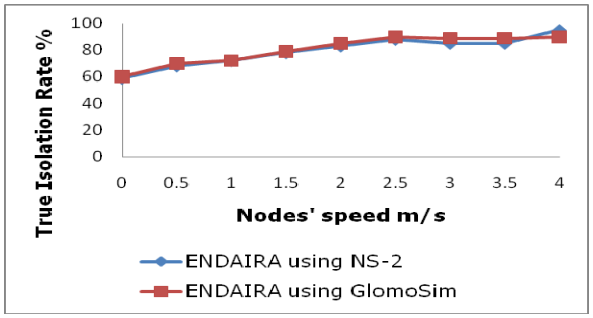

Figure 6. True Isolation Rate

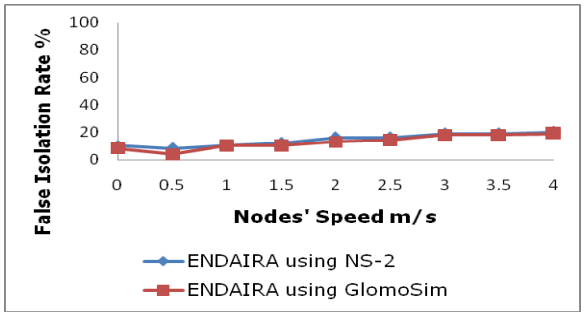

Figure 7. False Isolation Rate

Figure 7 shows that the false isolation rate has been considerably reduced when fixing optimally the parameters, and more importantly that the protocol becomes less affected with the mobility. The same pattern goes to these comparisons. The cost of this misbehavior detection is a small rise in end-to-end delay.

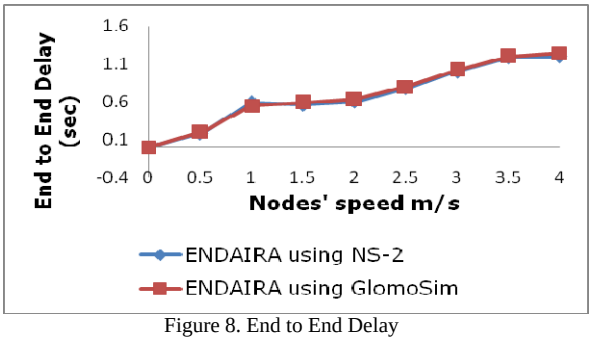

Figure 8. End to End Delay

For the delay, this is presented in figure 8, the small difference between ENDAIRA using GlomoSim and ENDAIRA using NS-2 protocols. This is basically due to cryptographic primitives (digital signatures computations on RREP packets) used by the launching of more route discoveries, thus more latency due to cryptography computation before sending the data packets. The most important issue here is the minor difference between ENDAIRA and our protocol. This difference is due to the monitoring procedures. From these results, it shows that

GlomoSim simulator is more suitable for ad hoc network. Also in implement the ENDAIRA routing protocol.

B. Phase 2: Results and Analysis

On phase 2 of the experiment will compare our basic ENDAIRA with NS-2 and previous secure routing protocol called ARIADNE. The analysis is shown in figure 9, 10 and 11.0. In term of comparison, we use the results of [2], ENDAIRA by using GlomoSim as the benchmarks.

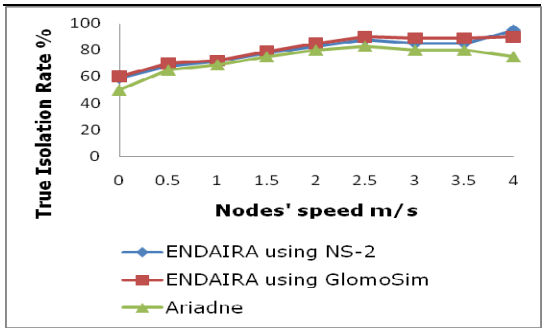

Figure 9. Comparing ENDAIRA with ARIADNE in term of True Isolation Rate

Figure 9 shows the percentage of true isolation rate for ARIADNE is low compared to ENDAIRA. At speed 3.5-4.0 m/s, the rates reduce drastically. This is because there are more nodes receive the route which is actually non-existent.

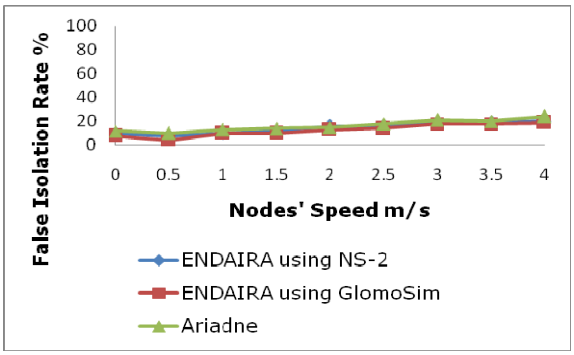

Figure 10. Comparing ENDAIRA with ARIADNE in term of False Isolation Rate

Since many nodes cannot verify the true route, the percentage of false isolation rate for ARIADNE is high compared to ENDAIRA.

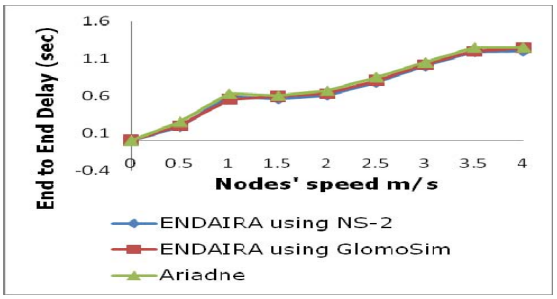

Figure 11. Comparing ENDAIRA with ARIADNE in term of End to End Delay

The delay also shows the comparison between ARIADNE and ENDAIRA as shown in figure 11 ARIADNE contributes higher delay than ENDAIRA. Communications, assigning MAC authentications between nodes takes more time to verify even though each node can't detect the present of adversary. Once the messages arrives to the destination, and get reply back with the routes which is does not exist, it will cause a problem especially when to verify the correct route after adversary has been detected. No one will confess which one is the correct route along the transmission.

VII. CONCLUSION

We demonstrated this by proposing a simulation based framework for on-demand source routing protocols that allows us to give a precise definition of routing security, to model the operation of a given routing protocol in the presence of an adversary, and to prove that the protocol is secure. We also proposed a new on-demand source routing protocol, ENDAIRA and made a comprehensive simulation study to first fix the crucial parameters of our solution to optimal values, and then to compared it with the basic protocols. As the future works, we would like to test and extend our research implementation in the real world which more exposed to the real attacks. This research also can be extending by measuring by more performance metric to prove that ENDAIRA is really the safety routing protocol to be used.

REFERENCES

[1] G. A´ cs, L. Buttya´n, and I. Vajda. Provable security of on-demand distance vector routing in wireless ad hoc networks. In *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, July 2005.

[2] Djamel Djenouri, Othmane Mahmoudi, Mohamed Bouamama, David Llewellyn-Jones, and Madjid Merabti. On Securing MANET Routing Protocol Against Control Packet Dropping. 2007.

[3] Todd R. Andel. Dissertation of Formal Security Evaluation of Ad Hoc Routing Protocols by the Florida State University, November 2007.

[4] L. Buttyan and I. Vajda. Towards provable security for ad hoc routing protocols. In *The ACM Workshop on Security in Ad Hoc and Sensor Networks SASN04*, Washington DC, October 2004.

[5] Gergely Ács, Levente Buttyán, István Vajda. Provable security for ad hoc routing protocols.2005.

[6] Gianni A. Di Caro. Dissertation of Analysis of simulation environments for mobile ad hoc networks by IDSIA / USI-SUPSI. December 2003.

[7] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). Internet RFC 3626, October 2003.

[8] P. G. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3, 2005, pp. 2-21.

[9] http://www.fedoraproject.com

[10] http://www.isi.edu/nsnam/ns/

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson. ARIADNE:: a secure on-demand routing protocol for ad hoc networks. In *The 8th annual international conference on Mobile computing and networking MobiCom '02*, pages 12–23. ACM Press, 2002.

[12] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *ACM Mobile Computing and Networking, MOBICOM 2000*, pages 255– 65, Boston, MA, USA, 2000.

[13] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *Proceedings of the ACM Symposium on the Theory of Computing*, 1998.

[14] D. Boneh, C. Gentry, H. Shacham, and B. Lynn. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology - Eurocrypt 2003*, Springer LNCS, 2003.

[15] www.ece.cmu.edu/~adrian/projects/secure-routing/ARIADNE.pdf

AUTHORS PROFILE

Ahmad Faisal Amri Abidin obtained his Master of Computer Science from Faculty of Computer Science and Information Technology, Universiti Putra Malaysia in 2008. Currently, he is a Lecturer at Department of Computer Science, Faculty of Informatics, Universiti Darul Iman Malaysia.

Nor Surayati Mohamad Usop obtained her Master of Computer Science from Faculty of Computer Science and Information Technology, Universiti Putra Malaysia in 2009. Currently, she is a Lecturer at Department of Information Technology, Faculty of Informatics, Universiti Darul Iman Malaysia.

Nurul Huda Nik Zulkifli obtained her Master of Computer Science from Faculty of Computer Science and Information Technology, Universiti Putra Malaysia in 2009. Currently, she is a Lecturer at Department of Communication Technologies, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.