International Journal of Computer Science and Informatics

Volume 2 | Issue 4 Article 12

April 2013

Flaws in Endair-A Secure Routing Protocol for MANETS

B. Swetha
Department of Computer Science, Vijay Rural Engineering College, Nizamabad, Andhra Pradesh, India, Swethalingannagari@gmail.com

S. Ajay Kumar
Department of Computer Science, Vijay Rural Engineering College, Nizamabad, Andhra Pradesh, India, ajay.sgr@gmail.com

TVS Prasad Gupta
Department of Computer Science, Vijay Rural Engineering College, Nizamabad, Andhra Pradesh, India, prasadgupta_tvs@yahoo.com

Flaws in Endair-A Secure Routing Protocol for MANETS

B.Swetha, S. Ajay Kumar & TVS Prasad Gupta

Department of Computer Science, Vijay Rural Engineering College, Nizamabad, Andhra Pradesh, India
E-mail : Swethalingannagari@gmail.com, ajay.sgr@gmail.com, prasadgupta_tvs@yahoo.com

Abstract **-** Routing is the one of the essential criteria at network level in mobile ad hoc networks. Ad hoc network routing protocols are difficult to design, and secure because unable to handle rapid node mobility and network topology changes. It has been realized by many researchers, and several "secure" routing protocols have been proposed for ad hoc networks. However, the security of those protocols has mainly been analyzed by informal means only. In this paper, we argue that flaws in ad hoc routing protocols can be very subtle, and we advocate a more systematic way of analysis. This approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but to the best of our knowledge, it has not. A new on-demand source routing protocol, called endairA, and demonstrate the usage of our framework by proving security. It is analyzed and shown that the security proof for the route discovery algorithm, endairA is flawed due to hidden channel attack. To overcome this flaw of EndairA algorithm, we uses acknowledgement based reply to find a secured route which provides more security and overcomes the hidden channel attack in the existing approaches.

Keywords **-** *Mobile ad hoc networks, hidden channel, provable security, routing protocols, secure routing.*

I. INTRODUCTION

A *Mobile Ad-hoc Network* is a multi-hop packet based wireless network composed of a set of mobile nodes, in which nodes assist by forwarding packets for each other to allow them to communicate and move at the same time, without using any kind of fixed wired infrastructure. It is self-organizing, rapidly deployable, adaptive and dynamic reconfigurable network of mobile nodes connected by wireless links. Node acts as host and router to support in transmitting data to other nodes in its range. MANET is differs from wired/wireless networks in that there is no central control, no base station, no access points and no wireless switches. It can be quickly and inexpensively set up as needed and it can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost.

There are numerous applications of MANETs, each having different characteristics such as network size (geographic range and number of nodes), rate of topological change, node mobility, communication requirements, and data characteristics. Applications such as military, disaster recovery and mine site operation, conferences, classroom, campus, may benefit from ad hoc networking, but secure and reliable communication is a needed prerequisite for these applications. Each node is directly connected to all nodes within it's possess effective transmission range and the communication among the nodes that are not within range of each other is accomplished by establishing and using multi-hop routes that involve other nodes which act as routers. New nodes can join the network at any time and existing nodes can leave the network as well.

Ad hoc network routing protocols are difficult to design, and secure because unable to handle rapid node mobility and network topology changes. Due to the dynamic nature of MANETs, designing communications and networking protocols for these networks is a challenging process. Routing in a MANET has two phases: route discovery and route maintenance. Route Discovery is the technique in which a node S intend to send a packet to destination D and get hold of a route to D. Route Maintenance is the mechanism in which node S is able to detect, while using a route to D and that have one or more links along the route have failed. When a broken link is discovered, the source can use another route or can revoke Route Discovery.

MANET routing protocols are generally classified into two types and they are proactive and demand based. Proactive routing continually maintains information on all available paths using periodic updates so when a

packet needs to be sent, routes are known and can be used immediately. The proactive method takes little time to discover routes but must maintain routing information for unused paths. Demand based routing, rather than maintaining paths between all nodes at all times, invokes a route discovery procedure on demand. Demand based schemes use less network bandwidth as they avoid sending unnecessary routing information but they typically take longer to discover routes.

On-demand routing protocols [1] have been demonstrated to perform better with significantly lower overheads than periodic or proactive routing protocols in many situations, since they are able to react quickly to the many changes that may occur in node connectivity, yet are able to reduce (or eliminate) routing overhead in periods or areas of the network in which changes are less frequent.

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. 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. The adversarial nodes may be connected through proprietary, out-of-band channels and share information.

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.

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.

In this paper, we focus on the area of secure routing protocols for ad hoc networks. First, given model describes the possible types of attacks in such a system and depict several new attacks on ad hoc network routing protocols. Second, present the design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called endairA, and demonstrate the usage of our framework by proving security. It is analyzed and shown that the security proof for the route discovery algorithm, endairA is flawed due to hidden channel attack. To overcome this flaw of EndairA algorithm, we uses acknowledgement based reply to find a secured route which provides more security and overcomes the hidden channel attack in the existing approaches.

II. ON-DEMAND SECURE ROUTING ALGORITHMS

Several researchers have proposed secure routing protocols. In that we have used many routing algorithm and all these secure routing protocols that have been proposed to reduce the risk of attacking the routing protocols.

Many secure routing protocols [10] aim to prevent the establishment of falsified routes. Security-Aware Ad hoc Routing (SAR) is 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. Here the data packets will be sent only through trusted nodes, with respect to the defined level.

1. ARAN Protocol:

Authenticated Routing for Ad-Hoc Networks (ARAN) is an on-demand, ad-hoc routing protocol that uses certificates to ensure authentication, message integrity, and non-repudiation of routing messages in an ad hoc networking environment. Based on logical route metrics and certificates, ARAN is immune to modification, impersonation, and fabrication of routing messages.

The ARAN[4],[8],[11] secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the ad hoc environment and consists of a preliminary certification process, a mandatory end to-end authentication stage and an optional second stage that provides secure shortest paths. ARAN requires the use of a trusted certificate server (T): before entering in the ad hoc network, each node has to request a certificate signed by T. The certificate contains the IP address of the node, its public key, a timestamp of when the certificate was created and a time at which the certificate expires along with the signature by T. All nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key.

The goal of the first stage of the ARAN protocol is for the source to verify that the intended destination was reached. As with any secure system based on

cryptographic certificates, the key revocation issue has to be addressed in order to make sure that expired or revoked certificates do not allow the holder to access the network.

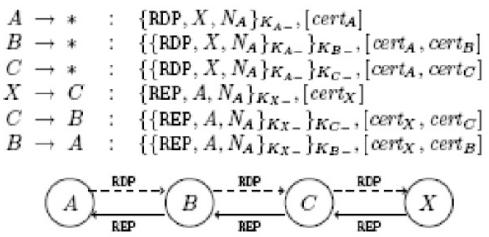

Fig. 2.1 : The ARAN protocol

(An example with 4 nodes)

In ARAN, when a certificate needs to be revoked, the trusted certificate server T sends a broadcast message to the ad hoc group that announces the revocation. Any node receiving this message rebroadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un-trusted node. This method is not failsafe.

In some cases, the un-trusted node that is having its certificate revoked may be the sole connection between two parts of the ad hoc network. In this case, the non-trusted node might not forward the notice of revocation for its certificate, resulting in a partition of the network, as nodes that have received the revocation notice will no longer forward messages through the un-trusted node, while all other nodes depend on it to reach the rest of the network. This only lasts as long as the un-trusted node's certificate would have otherwise been valid, or until the un-trusted node is no longer the sole connection between the two partitions. At the time that the revoked certificate should have expired, the un-trusted node is unable to renew the certificate, and routing across that node ceases. Additionally, to detect this situation and to hasten the propagation of revocation notices, when a node meets a new neighbor, it can exchange a summary of its revocation notices with that neighbor; if these summaries do not match, the actual signed notices can be forwarded and re-broadcasted to restart propagation of the notice.

2. SAODV Protocol:

Mobile ad hoc networks are vulnerable to various security threats because of its dynamic topology and self configurable nature. SAODV (Secure Ad hoc On Demand Vector routing) is an implementation of SAR on AODV. It is one of the popular secure mechanisms which take the help of digital signature and hash chain techniques to secure AODV packets. Since, digital signature technique consumes heavy computational time, the degradation of SAODV performance can be a major issue. In a recent work called A-SAODV (Adaptive SAODV), an adaptive mechanism that tunes the behavior of SAODV improves its performance.

In this paper we have proposed an extension to Adaptive SAODV of the secure AODV protocol extension, which includes further filtering strategies aimed at improving its performance. Moreover, we analyze how our proposed algorithm can help to further improve the performance of adaptive SAODV. One of the problems 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.

3. SRP Protocol:

Source routing protocols (SRP) is an on-demand secure source routing protocol that captures the basic features of reactive routing. It prevents spoofing attacks. This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length. Route requests generated by a source S are protected by MACs computed using a key shared with the target T. Requests are broadcast to all the neighbors of S. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link.

4. Ariadne Protocol:

ARIADNE [7],[8] (A Secure On-Demand Routing Protocol for Ad Hoc Networks) is an on-demand secure adhoc routing protocol based on DSR that withstands node compromise and relies only on highly efficient symmetric cryptography. ARIADNE guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to the destination present in the RREP message and that no intermediate node can remove a previous node in the node list in the RREQ (Route Request) or RREP (Route Replay).

Operation:

As for the Secure Routing Protocol (SRP), protocol ARIADNE needs some mechanism to bootstrap authentic keys required by the protocol. In particular, each node needs a shared secret key (KS, D) is the shared key between a source S and a destination D with each node it communicates with at a higher layer, an authentic TESLA key for each node in the network and an authentic "Route Discovery chain" element for each node for which this node wi ll forward RREQ messages.

Features:

(i) ARIADNE provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties.

(ii) For authentication of a broadcast packet such as RREQ, ARIADNE uses the TESLA broadcast authentication protocol.

(iii) Selfish nodes are not taken into account.

Strengths:

(i) ARIADNE copes with attacks performed by malicious nodes that modify and fabricate routing information, with attacks using impersonation and, in an advanced version, with the wormhole attack.

(ii) ARIADNE is protected also from a flood of RREQ packets that could lead to the cache poisoning attack. (iii) ARIADNE is immune to the wormhole attack only in its advanced version: using an extension called TIK (TESLA with Instant Key disclosure) that requires tight clock synchronization between the nodes; it is possible to detect anomalies caused by a wormhole based on timing discrepancies.

5. Security-Aware Ad-Hoc Routing (SAR):

Security-Aware Ad-Hoc Routing (SAR)[2] is the generalized framework for any on demand ad-hoc routing protocol. SAR requires that nodes having same trust level must share a secret key. SAR augments the routing process using hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity while the encryption of packets ensures their confidentiality**.**

6. Secure Link State Routing Protocol SLSP:

Secure Link State Routing Protocol (SLSP) provides secure proactive topology discovery and can be used as either as a stand-alone protocol or as a part of Hybrid routing framework when combined with a reactive protocol.

7. ABV Model:

The ABV model [1],[2],[4],[6],[7] is a security framework proposed by Acs, Buttyan and Vajda[1] used to analyze on-demand routing algorithms, SRP and Ariadne and finds them insecure against hidden channel attacks. ABV proposed to merge faulty neighbor nodes into a single node. So the neighbor nodes of a faulty node on a route are not faulty. Consequently, adversarial nodes are, by definition, never adjacent in the ABV model. This is an arbitrary restriction that greatly limits the scope of the security statements in the ABV model in their ability to capture realistic security requirements.

However, this model is not left to identify a problem with the security proof of endairA. So, for the sake of argument, we also assume that adversarial nodes are never adjacent. This implies that the route can be uniquely partitioned as follows: each partition consists of a single non compromised identifier or a sequence of consecutive compromised identifiers.

It is concluded that the proof makes the unwarranted assumption that no direct channels imply no direct bandwidth between adversarial nodes; the proof is therefore incomplete. It could be possible that the security claims remained valid even as their proof is incorrectly argued. Fundamentally, endairA and the ABV model was developed to deal with a class of hidden channels, the intrinsic hidden channels of a wireless broadcast medium in a neighborhood. However, security is not achieved because other hidden channels remain present.

III. MODELING ENDAIRA PROTOCOL:

Inspired by Ariadne with digital signatures, a routing protocol is designed that can be proven to be statistically secure. The protocol is called as endairA, which is the reverse of Ariadne because instead of signing the route request, it is proposed that intermediate nodes should sign the route reply.

The route request format of EndairA is,

$$Msg_{S,T,rreq} = (rreq,S,T,id,X_1 \ldots\ldots X_j)$$

The route reply format of EndairA is,

$$Msg_{S,T,rrep}=(rrep,S,T,id, X_1 \ldots X_p, sig_{T,\ldots.} \quad sig_{Xj})$$

Each intermediate node also verifies that the digital signatures in the reply are valid and that they correspond to the following identifiers in the node list and to the target. If these verifications fail, then the reply is dropped. Otherwise, it is signed by the intermediate node, and passed to the next node on the route towards the initiator. When the initiator receives the route reply, it verifies if the first identifier in the route carried by the reply belongs to a neighbor. If so, then it verifies all the

signatures in the reply. If all these verifications are successful, then the initiator accepts the route.

Analysis of EndairA:

The protocol, EndairA is claimed to be proven secure in the ABV security framework. The proof of security of endairA is revisited and flaw is identified. The proof considers the possibility of an attack against endairA being successful, hoping to achieve a contradiction. However, Acs, Buttya´n, and Vajda exclude such faulty routes which may appear shorter than actual network routes by collusion of adjacent adversarial nodes by subsuming all adjacent adversarial nodes.

A plausible route is one whose partitions correspond to that of a real route that physically exists in the network. The security statement of endairA is that it only accepts plausible routes. Note that this statement also does not consider an adversarial lengthening of a route by assignment of multiple labels to a single compromised network node as an attack.

EndairA algorithm proposed by ABV is analyzed and shown that the security proof for the route discovery algorithm for endairA is flawed due to hidden channel attack. To overcome the flaw of EndairA, we uses acknowledgement based reply to find a secured route, which provides security and overcomes the hidden channel attack. We uses hash based technique in which, whenever a source sends its route request to its neighbors, the neighbor node which receives the route request send an acknowledgement based reply that it has received the route request and hence it avoids the presence of faulty nodes by which the source receiving the identity of every node in the network and hence the network is more secure without malicious nodes. Therefore the route discovered is secure. It is concluded that the proof makes the unwarranted assumption that no direct channels imply any direct bandwidth between adversarial nodes; the proof is therefore incomplete.

$$
\begin{array}{lcll}
A & \longrightarrow & * & : \ \mathtt{RREQ}, A, X, id, [\,] \\
B & \longrightarrow & * & : \ \mathtt{RREQ}, A, X, id, [B] \\
C & \longrightarrow & * & : \ \mathtt{RREQ}, A, X, id, [B, C] \\
X & \longrightarrow & C & : \ \{\mathtt{RREP}, A, X, [B, C]\}_{K_{X-}} \\
C & \longrightarrow & B & : \ \{\{\mathtt{RREP}, A, X, [B, C]\}_{K_{X-}}\}_{K_{C-}} \\
B & \longrightarrow & A & : \ \{\{\{\mathtt{RREP}, A, X, [B, C]\}_{K_{X-}}\}_{K_{C-}}\}_{K_{B-}}
\end{array}
$$

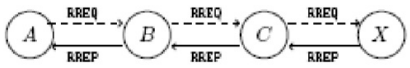

Fig. 2.2 : The endairA routing protocol

An attack on Endair A:

This is a hidden channel attack that does not require out-of-band resources. Consider an instance of endairA with source node S and let, (S, A, X, B, A, D, T) be a sequence of identifiers of pairwise neighbor nodes in which only X; Y are faulty.

In the attack, when the second faulty node Y receives,

$msg_{S,T,rreq=}$(rreq, S, T, id, A, X, B)

It drops node B from the listing and transmits,

$msg_{S,T,rreq=}$(rreq, S, T, id, A, X, Y)

Eventually, the route request will reach the target T, which will compute and send back a route reply. Node Y will then receive from D,

$msg_{S,T,rreq=}$(rreq,S,T,id,A, X, Y, D, sig_T,sig_D)

Now, Y can obviously attach its label and signature to this reply and transmit to B the extended reply, but B will not retransmit it because B is not included in the listing. However, suppose that Y had earlier received a request from D to find a route linking it to A.

IV. ROUTING DISCOVERY:

The process of routing discovery is like DSR which only some security considerations. Routing discovery means data moves from source to the destination. Data transfer from source to the destination, Behavior in case of error

1st Solution: The CONFIDANT Protocol

Idea: punish non collaborative/malicious nodes by non-forwarding their traffic.

Detection through “neighborhood watch”

Building a distributed system of reputation

Enable “re-socialization” through timeouts in the black list.

2nd Solution: Nuglets

Idea: virtual currency to buy the collaboration Nuglets are attached to the message

Each relaying node takes nuglets form the message which can use to buy the routing of its own message

Nuglet module must be implemented in a tamper resistant hardware to avoid cheating.

3rd Solution: Securing Routing Information

Idea: share the routing information through a secure channel

Requires Key Managementand Security Mechanisms

V. CRITICAL APPRAISAL

Key Setup

- Methods : Pre-deployed, KDC, CA
- Fixed nodes. Circular dependency.
- Centralized

FIXED NODES IN SOME CONDITIONS

- Circular dependency
- Resource constrained. Insecure

MAXIMUM END-TO-END DELAY

- How to choose adaptively

HIDDEN CHANNEL ATTACKS INTERMEDIATE NODE AUTH EN-TICATION

- Authentication on demand

REMAINING SECURITY ISSUES

- Passive eavesdropper
- Inserting data packets attack
- Non-participating attacker
- Single layer security scheme

MAN-IN-THE MIDDLE ATTACKS FORMAL SECURITY MODEL DELAY AND BUFFER SIZE

- Slow responsiveness
- Resource constrained

VI. CONCLUSION

Based on the ABV model, a new security framework tailored for on-demand route discovery protocols in MANETs was proposed. A new on-demand source routing protocol, called endairA, and demonstrate the usage of our framework by proving security. It is analyzed and shown that the security proof for the route discovery algorithm i.e. EndairA which represents formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks, the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. This provides efficient security to the mobile ad hoc network and there is no possibility for hidden channel attack and the route discovered is highly secured.

REFERENCES

[1] G.Acs, L. Buttya´n, and I. Vajda, “Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks”.

[2] P. Papadimitratos and Z. Haas, “Secure Routing f or Mobile Ad Hoc Networks”.

[3] G. Acs, L. Buttya´n, and I. Vajda, “Provably Sec ure On-Demand Source Routing in Mobile Ad Hoc Networks”.

[4] G. Acs, L. Buttya´n, and I. Vajda, “Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks”.

[5] M. Burmester, T. van Le, and A. Yasinsac, “Adaptive Gossip Protocols: Managing Security and Redundancy in Dense Ad Hoc Networks”.

[6] L. Buttya´n and I. Vajda, “Towards Provable Security for Ad Hoc Routing Protocols”.

[7] Y.-C. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks”.

[8] Y.-C. Hu, A. Perrig, and D. Johnson, “A Survey o f Secure Wireless Ad Hoc Routing Protocols”.

[9] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”.

[10] 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.

[11] B. Dahill, B. N. Levine, E. Royer, and C. Shields. Aran:A secure routing protocol for ad hoc networks. TechnicalReport UMass Tech Report 02-32, University of Massachusetts, Amherst, 2002

◈◈◈