ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Secure MANET Route Discovery Framework

D.Sowmya[1], J.Kiran Kumar[2], M.V.S.S. Nagendranath[3]

#1 Student, Sasi Institute of Technology and Engineering, Tadepalligudem,W.G(dt)

#2 Asst.professor, Sasi Institute of Technology and Engineering,Tadepalligudem,W.G(dt)

#3Assoc.professor, HOD,Sasi Institute of Technology and Engineering, Tadepalligudem,W.G(dt)

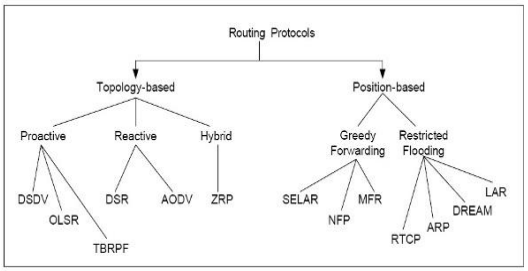
Abstract: Data relaying is a crucial component in Mobile ad hoc networks (MANETs) communications as they experience restricted broadcast range, resources and with no fixed infrastructure. Node collaboration is vital for relaying and very few protocols in MANET support it. Speed and Security are the metrics to be considered while initiating route discoveries during node collaborations. Prior approaches ability to incorporate these metrics into Source Routing Protocol (SRP), endairA protocol of MANETS, the challenge lies in maintaining these metrics until the duration of the entire process of route discovery. So instead of protocol initiations we propose to develop and deploy a security framework derived from modified endairA for MANETS with respect to compos ability factors like adversary models, communication medium, and payload and secure sockets layer management. The performance of this framework is helpful in achieving faster and secure route discoveries during communications and a practical implementation of the proposed framework validates our results.

Keywords—Routing protocols (security), Network architecture and design—distributed networks (security), MANET security, hidden channels, route lifetime, routing failures, routing overhead, packet delivery ratio.

I INTRODUCTION

The Mobile Ad hoc Network (MANET) consists of many mobile nodes with wireless communication that can communicate with each other without any physical infrastructure, so it is called as infrastructure less network. The power exhaustion of some nodes and the mobility nature of nodes cause frequent topology changes. So the path between nodes or group of nodes may change continuously.

The node which want to transmit data packets, first needs to discover the route to the destination using route discovery process of different routing protocols. There are two kinds of routing protocols, one is reactive or on-demand routing protocol, and another is proactive or table-driven routing protocol.



Also the routing protocols are needed to be protected from possible internal and external attacks to avoid malicious or compromised nodes to be involved in the route discovery process. The malicious nodes cause in dropping of routing packets without forwarding to destination, sending false route information with expected QOS parameters and discarding the data packets. The security may be provided either using the traditional cryptographic mechanisms; such as digital signature and public key encryption or we can provide reputation based security. But both methods have its own pros and cons.

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

The cryptographic based secure routing requires a key management service to keep track of key and node binding. Traditionally the key management service is based on a reputation of the entity called a certificate authority (CA) to issue public key certificate of every node. Also every intermediate node needs to encrypt and decrypt the control packets before forwarding it to the next hop neighbor nodes during route discovery phase which involves more computational overhead.

In the reputation based secure routing, the reputation of every node is calculated by considering the knowledge, experience and recommendation of that particular node's immediate neighbor nodes based on a particular node's communication and behavior with its neighbor node. Every node maintains the reputation value of its one hop neighbor in the reputation table. This reputation value is a dynamic value. So we need to calculate the reputation value periodically, and update the new values with the old value in the reputation table.

Due to mobility nature, more computations involved in the route discovery process and the power constraint of the nodes , a host may exhaust its power or move away without giving any notice to its cooperative nodes which causes network topology changes. These changes may significantly degrade the performance of the routing protocols. So the route needs to be discovered with longest route lifetime with less mobility nature. As the route consists of the number of wireless links, the route lifetime depends on the node life time and individual links lifetime. The route discovery without considering the lifetime of the route leads to frequent route discovery and computation overhead of nodes.

The multipath route discovery concept reduces node's computational overhead by discovering multiple paths for a single route request. If a single path fails, the alternate path can be used without reinitiating a new route discovery process. Thus the security threats and dynamic topology of ad hoc network nodes make the designing of the routing protocol for MANET very difficult. This also results in frequent path breaks and frequent route discovery and node computation overheads. So MANET routing protocols should be designed without any security threats and also the lifetime of the route, reputation of the route need to be considered as the routing metrics in order to reduce the number of route discovery processes and also to improve network performance.

II RELATED WORK

2.1 Several route discovery algorithms have been proposed in the literature (see, e.g., [1], [2], [3], [4], [5]). These focus mainly on efficiency issues such as scalability with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements. Some of the proposed routing algorithms also address security issues (e.g., [6], [7], [8], [9], [10], for a survey, see [11]), but their security is restricted to rather weak adversary models. There are several reasons for this, the most important one being that it is hard to model a formal security framework that captures all the basic security aspects of a MANET. Several attempts have been made to address the security of MANET route discovery more robustly, the most recent one being introduced in a series of papers by Buttya`n and Vajda [12] and Acs et al. [13], [14], [15], [16]. In these works, the authors develop a formal idealization and simulation framework that adapts ideas from the secure reactive systems approach [17] and universally composable security approach [18] to the realm of MANET applications. One of the advantages of the new approach—which we will refer as the ABV model—is that it highlights security issues related to concurrent protocol executions. Indeed, the authors of the ABV model prove that, within their model, the routing algorithms SRP [3] and Ariadne [15] are insecure and subject to a hidden channel attack. A solution is then proposed in the form of a novel route discovery algorithm, named endairA—the name reflects the fact that it applies security primitives in the reverse order of the Ariadne protocol—and a proof is also supplied for the claim that endairA is secure in the ABV model [15].

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

2.2 Ariadne: ARIADNE [9],[10] (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 will 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.

2.3 ABV Model: The ABV model is a security framework proposed by Acs, Buttyan and Vajda[14] 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.

III PRELIMINARIES

EndairA Protocol: Inspired and derived from 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,

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

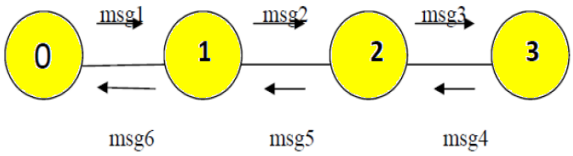


Fig:1. EndairA Protocol Message

msg1=(rreq,0,3,id,())
msg2=(rreq,0,3,id,(1))
msg3=(rreq,0,3,id,(1,2)) msg4=(rrep,0,3,(1,2),(sig3))
sig3=sk3{rrep,0,3,id,(1,2),()}
msg5=(rrep,0,3,(1,2),(sig3,sig2))
sig2=sk3{rrep,0,3,(1,2),(sig3)}
msg6=(rrep,0,3,(1,2),(sig3,sig2,sig1))
sig1=sk1{rrep,0,3,(1,2),(sig3,sig2)}

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

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.

An attack on EndairA: 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 pair wise 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 Framework using modified EndairA

Each node maintains a flow table, which stores a $flow_{ID}$, a flow counter ($flow_c$) and the ID of the previous node from the data is received (BID). The $flow_{ID}$ is the concatenation of the source, destination ID's of a particular flow and the node of the previous hop node, which has forwarded the packet (i.e. $flow_{ID}$ = $S_{ID}|B_{ID}|D_{ID}$). This strategies allows each node to independently assign unique flow IDs and identify all data flows travelling through or originating from them. The flowc stores the number of different unique data flows that pass through each node. This includes the data flow in which the nodes act as an intermediate node and the data flows that they initiated. Note that the data flow tables maintain information about flows, which are considered as active. To do this, each node updates its data flow counter periodically using timeouts and also reactively when a broken link is reported. Similarly, new flows are added reactively, when a nodes initiates or forwards a data packet which is recorded in the flow table. The following algorithms illustrate optimization required EndairA.

Algorithm

1. $Flow_t$ Flow expiration time
2. $Flow_{ID}$ Flow ID for the data packet
3. $Flow_T$ The flow table
4. $Flow_c$ Flow counter
5. $Flow_A$ Flow Update Flag
6. S_{ID} Source node ID
7. D_{ID} Destination node ID
8. B_{ID} Previous forwarding node ID
9. $Flow_{ID}$ = $S_{ID}|B_{ID}|D_{ID}$
10. Found False A flag used to find Flow ID
11. for i← 0, i < $Flow_c$, i + +
12. if $Flow_T$ [i]:$Flow_{ID}$ = $Flow_{ID}$
13. Found True
14. break
15. if Found = True
16. Set($Flow_T$ [i]:$Flow_t$)
17. else
18. $Flow_T$ [i]:$Flow_{ID}$ ← $Flow_{ID}$
19. $Flow_T$ [i]:B_{ID} ← B_{ID}
20. Set($Flow_T$ [i + 1]:$Flow_t$)
21. $Flow_c$ + +
22. if $Flow_c$ >= 1 & $Flow_A$! = Active

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

23. $Flow_A$ Active
24. Activate the Flow-Delete-Proactive function

V PERFORMANCE

Computational cost of the proposed protocol is measured, separately, at source, intermediate and target nodes,based on the number of energy intensive operations involved during the route discovery process. Here, based on the result of [19], we consider signature generation, verification and scalar multiplication operations which are energy intensive. Based on our performance analysis, we have compared the computational overhead at source, intermediate and target nodes for the proposed protocol, with respect to Ariadne and EndairA and the results are shown in following graphs.

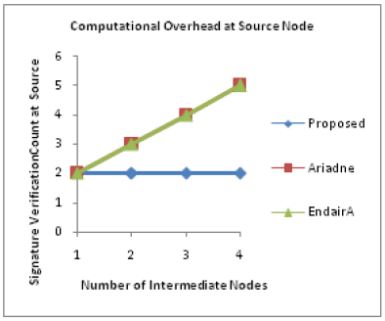


Figure 5.1: Computational overhead at source node

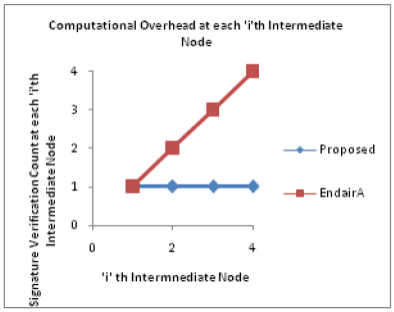


Figure 5.2: Computational overhead at intermediate node

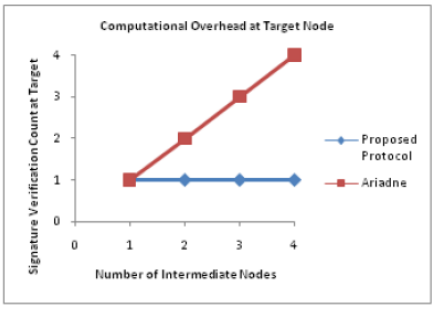


Figure 5.3: Computational overhead at target node

VI CONCLUSION

We propose to develop a new security framework customized for reactive route discovery protocols in MANETs extended from EndairA protocol. This framework is a formal security model that can deal with route manipulation attacks at intermediaries and is successful in mitigating a special class of hidden channel attacks. These attacks are intrinsic nature with respect to the wireless broadcast medium in a adhoc network neighborhood. In the context of mobility, which requires that route discovery take place concurrently with data transmissions, extra bandwidth is available to adversarial nodes that should be nullified by faster updates about routes during node collaboration. Handling nonexistent links is still an open issue that can be considered in a future research.

VII REFERENCES

[1] Mike Burmester and Breno de Medeiros, On the Security of Route Discovery in MANETs, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 9, SEPTEMBER 2009

[2] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, eds., Kluwer Academic Publishers, 1996.

[3] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02), 2002.

[4] C. Perkins, "Ad-Hoc On-Demand Distance Vector Routing," Proc. Military Comm. Conf. (MILCOM '97), panel on ad hoc networks, 1997.

[5] C.E. Perkins and E.M. Belding-Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. Second Workshop Mobile Computing Systems and Applications (WMCSA '99), pp. 90-100, 1999.

[6] M.G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing," Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 106-107, 2002.

[7] P. Papadimitratos and Z. Haas, "Securing Mobile Ad Hoc Networks," Handbook of Ad Hoc Wireless Networks, M. Ilyas, ed., CRC Press, 2002.

[8] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '02), pp. 78-89, 2002.

[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, 2003.

[11] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy, vol. 2, no. 3, pp. 28-39, Mar. 2004.

[12] L. Buttya´n and I. Vajda, "Towards Provable Security for Ad Hoc Routing Protocols," Proc. ACM Workshop Ad Hoc and Sensor Networks (SASN '04), 2004.

[13] G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," Technical Report 159, Int'l Assoc. for Cryptologic Research, 2004.

[14] G. Acs, L. Buttya´n, and I. Vajda, "Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks,"Proc. European Workshop Security and Privacy in Ad Hoc and Sensor Networks (ESAS '05), pp. 113-127, 2005.

[15] G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[16] G. Acs, L. Buttya´n, and I. Vajda, "Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks,"Proc. Workshop Security in Ad Hoc and Sensor Networks (SASN '06), pp. 49-58, 2006.

[17] B. Pfitzmann and M. Waidner, "Composition and Integrity Preservation of Secure Reactive Systems," Proc. ACM Conf. Computer and Comm. Security, pp. 245-254, 2000.

[18] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Proc. IEEE Ann. Symp. Foundations of Computer Science (FOCS '01), pp. 136-145, 2001.

[19] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols," IEEE Transactions on Mobile Computing, vol. 5, pp. 128-148, 2006.