ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A Comparison on ARAN and SAODV Protocols of Ad-hoc Network Routing

Ali Tourani[1], Yasin Ezatdoost[2], Amir Seyed Danesh[3]

Department of Computer Engineering, University of Guilan, Iran [1]

Department of Computer Engineering, University of Guilan, Iran [2]

Faculty of Computer Science and Information Technology University of Malaya, 50603, Kuala Lumpur [3]

Abstract: Today's Ad-hoc networks have various applications in human life but always face numerous challenges as a result of node mobility and high faking possibility. One of the min challenges of Ad-hoc networks is the correct and suitable routing. In order to achieve the best suited track the networks use various protocols. But, what are sought in these protocols are a authenticates routing and developing confidence and trust in them of which ensuring meeting correct node by correct data or receiving from an identified node is an important part. The present paper aims at investigating available protocols in Ad-hoc networks besides exploring ARAN and SAODV authenticates routing protocols and their costs and determining the most suitable and optimal protocol.

Keywords: Ad hoc Network, ARAN Protocol, SAODV Protocol, Ad hoc Protocols.

I. INTRODUCTION

As their name represents, Ad-hoc networks are predicted and designed for use in emergencies [1]. These networks highly differ in node type, routing and application with structured networks. In Ad-hoc networks, nodes do not use a certain and intensive structure to communicate and lack an integrated and regular management [2] but perform same tasks based, only, on a certain algorithm. Moreover, their node types (both middle and end nodes) oppose those of other networks [3]. Among essential applications of such networks are in military environments in order to communicate in war conditions, environmental applications such as being used in forests as fire sensor and in mobile communication networks [10].

II. CHALLENGES AND WEAKNESSES

Since all Ad-hoc networks need wireless technology for communication ensuring their security and safety is always a main issue of concern. As a node-to-node transfer is required for moving data from an origin to a specific destination vast errors are expected as a result of using wireless networks and lack of management [3]. Followings are some main weaknesses of Ad-hoc networks:

- Lack of node control: impossibility of validation in the structure of Ad-hoc networks and lack of intensive access
- Processes of each node: some weaknesses of the network originate from imposing numerous processes on every node during routing [5]
- Wireless network: high possibility of destructive attacks, eavesdropping, destruction of sent data and fake identity of destructor nodes
- Dynamic topology:
- Lack of a stable and secure link because of frequent entering and abandoning network nodes
- Limited resources: short lifecycle of nodes
- Common channel of data transfer: vulnerability of a single radio channel in the network
- Security problems of assigning keys to nodes [6] [11]

These weaknesses exist in the context and body of features of Ad-hoc networks and are never disappeared but they can be managed so that they impose the lowest harm on network security. In addition to security there is another important challenge in Ad-hoc networks: making use of suitable algorithms in order to find the best origin-to-destination track while having least expenditures since the networks have nodes with short life-cycle. Hence, parsimony in routing of every node and reduction in its processes maximum logical use can be made of every certain node.

Assembly of these important challenges causes a comprehensive challenge called "authenticates routing" [13] [14]. Here, the network is expected to impose the least processes on every node, find the best track, and check node functionality, etc. while appealing authenticates operations in the network. Security includes various essential factors such as availability of nodes, confidence, authentication and integrity [15].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

III. ROUTING ALGORITHMS

As mentioned earlier routing in Ad-hoc networks is performed by nodes. Network nodes lack sufficient knowledge on topology of the available network and hence have to find the location of destination in the network (for every sending process) in order to be able to communicate other nodes. In fact, each node which joins the network first broadcasts its presence in the network among other nodes and then waits for a neighbour's reply and, thus, gains information about its adjacent nodes [7] [8].

Routing is performed in a variety of ways in these networks:

- Flooding method: in which the node first sends its data to all neighbouring ones and then, very node receiving the data copies it and sends it to other adjacent nodes. Therefore, the destination node and the track (path) toward it are identified.
- Gossiping method: in his method (a simplification of flooding method) data is sent to a neighbour randomly in every certain step [16].
- Directed dispersion: is used to find an efficient rout between the sender and receiver and is more complicated than other methods.
- Rotating method: is widely used to effectively disperse data in sensor networks. In this method every certain node can make decisions in every step based on effective communication.

Ad-hoc networks have numerous routing protocols. Table Driven Routing protocol, One-Demand Routing protocol, Flow Oriented Routing protocol, etc. [22] are some examples. But, what we consider here is to design protocols for secure routing in Ad-hoc networks. To common and mostly used protocols in this area are ARAN and SAODV which are compared and discussed below.

IV. A COMPARISON ON ARAN AND SAODV PROTOCOLS

A. Authenticated Routing Protocol (ARAN)

ARAN is a routing algorithm used in Ad-hoc networks and works based on AODV model [an alternative of on-demand routing protocol). The invader is always possible in this protocol to investigate the network traffic and nodes. The required feature of operational environment (in ARAN) is so that the routing signalling must not be prone to e faked by invaders and it is not also possible to send invalid routing data outside the network [17] [18]. Moreover, the selected route should not pass a signalling node before full identification. There are certain resources in the structure of ARAN which enable assigning an ID or presence certificate to the network. All nodes in the network know this certificate (labelled CA) and if a node is going to enter the network, it must receive a key from the source. The certificate includes four specific IP addresses of the new node, the public key of the node and issuance and expiration date of the certificate [19]. The data is finally coded by the private key and presented to the new node as a package in the form of its presence certificate.

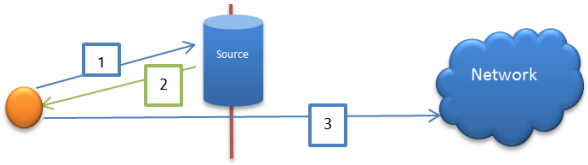

Fig. 1 how a node is added to the network: 1) applying for entrance by the new node, 2) assigning presence certificate to the node by source, 3) allowing the new node to enter the network

If a node (S) is going to develop a route to another node (d) it must first send a request package for all its neighbouring nodes. The package contains request phrase, destination IP address, serial number of the request package and the layer coded by private key of the origin node. Every node receiving the package first verifies a node in the network by exploring its certificate and then determines its route request by assessing available serial numbers and IP addresses. If the present node has not already received the package (lack of infinite loop) it codes the content of received package again (through its own private key). This is called "signature" [20].

Fig. 2 in this figure the green package is the one sent from origin and the purple is the package signed by the neighbouring node (having confirmed the identity and infrequency)

Similarly, when the package meets the next node, the node investigates it and replaces its own public and private keys with those of previous step (if the package is confirmed). In fact, it erases the signature of previous node and replaces its own.

Now, imagine that the package arrives at the destination. In this case the destination node authenticates the package. Then, having received an assigned pack it generates a new package through which it sends the newly received package. The new package (reply pack) is similar to the request pack and has a destination IP address (requesting node), new serial number, its own public and private keys and reply text. When the package is sent, all receiving nodes perform an operation similar to that of taking the package to its destination. This process continues until the package meets requesting node. In this way the requesting node finds out that there is a suitable and secure route toward the identified destination node. The route is called authenticated (secure) and reliable since the received package is explored and identified in every step and a node out of the network cannot have any receive [21]. Besides, it is possible to trace the invader node because of a fake signature. On the other hand, since the node signature is needed the package content does

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

not change. Hence, three security features (confidence, integrity, and authentication) are met.

The protocol has disadvantages and deficiencies despite above specifications. One of the main weaknesses of ARAN method is that it bases upon asymmetric coding and electronic signature and hence it is vulnerable to attacks such as Dos. Furthermore, asymmetric coding is a complicated task and it is costly and time consuming to use it in each step of send and receive. As nodes of this network require low costs and limited resources the method is not considered fitted in terms of resource consumption. Moreover, if the performance of CA is influenced by every known or unknown factor the ability to communicate other nodes is affected since the algorithm is highly dependent on the CA. Another deficiency of this pattern is its high vulnerability to Worm-hole attacks (because of slow performance) and Rushing attack (because of requiring time for decision making) [24].

ARAN protocol is a hop-to-hop authenticated routing protocol and requires signature investigation in every step. An interesting feature of ARAN is dividing receivers to "close" and "far away" groups. Nodes having requests and replies from the source node with one-hop distance are classified in the first group and those with several-hop distances in the second. This feature is used in cost estimation.

B. Secure Ad-hoc on-demand distance vector (SAODV)

Besides ARAN, SAODV is another secure routing algorithm designed based on AODV (which makes it secure and optimal). In this algorithm the protocol first divides routing package into two sections. One section contains a part of the package which changes along the route and the other includes the part which remains stable. In order to ensure package security the first section uses Hash codes and the second employs coding through the public key. Hash codes of jump number are required to prevent data manipulation and alteration. To do this, the origin node first generates a random link and Hashes is it TTL times (TTL is the highest number of allowed jumps for a package) and finally embeds it in the Header of pack and sends it. On the other hand, the Hash chain (which is developed through using the random link and hashing it in every jump) is added to the Header. Now, as soon as a node receives the sent package it explores whether the two links added to Header arte equal. If they are equal, the receiver node confirms accuracy of jump number, increases it for 1 unit and sends it again having performed interfusion (Hashing).

The objectives of using SAODV protocol include:

- Stabilizing the moving data along the route
- Authenticating the origin node
- Confirming data accuracy by routing package

Similar to ARAN this protocol uses electronic signature. The sender node signs the package before sending and other nodes only validate it along the route. Having the package received the destination node generates a reply package and sends it after signing whit its own private key [26]. In SADOV protocol middle nodes have access to the considered private key in order to enable generation of reply to route request packages (embedded in ADOV) [27]. Therefore every middle node adds the remaining expiration date of the route to the package and signs it with private key of destination node and its own private key. At last, the assembled package is sent in the reverse route.

Resistance against Dos, Black-hole and gray-hole attacks, inability of nodes outside the network in sending route request package, limiting middle groups' activity to increasing jump number are among considerable advantages of SADOV. Some of its disadvantages include unsafe availability of nodes' private keys to other nodes, possibility of MIM attacks by invader nodes, possibility of simulation (fake) adjacency feature by the invader node while sending reply message [28].

V. A COMPARISON ON ARAN AND SAODV PROTOCOLS

As mentioned earlier costs in ARAN are estimated by dividing nodes into two (close and far away) groups. So, two signatures are required for close nodes: one to specify he source and the other to obtain the public key, while far away node require 4 signatures. But, SAODV suggests two types of signatures: one is a single signature (in which only the node responding to REP is the destination node) and the other is a dual signature. All signatures must use Hash functions to be considered by the new Hop unless the node itself is the source of REP or REQUEST, a case in which signature development has some costs. In general, when a node sends a routing request or routing reply the protocol develops a random figure named "seed" and puts its value in the Hash field. It also puts zero for hop-count field and surplus TTL of the IP package for MAX $_{\text{hop-count}}$ field. Then Hashes the value of Seed as much as that in hop-count$_{max}$ field. The resulting value is called "top-ash". On the other hand, when a node receives a request first Hashes it for MAX $_{\text{hop-count}}$ times. If the value equals that of top-hash, it is then confirmed. Generally, costs of the two protocols can be summarized as Table I.

TABLE I
COSTS OF ARAN AND SAODV PROTOCOLS

2(N-4)(S+4S') + 2(S+2S') + 2 (S+4S') + (S+4S')	CostARAN
2S + H(Max $_{\text{hop-count}}$ – hop-count)	CostSAODV

In estimating costs of ARAN values of S, 4S' and 2S' are costs of current signature, investigating far node and investigating close node, respectively and N is number of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

nodes between origin and destination. A single-signature is used to estimate costs of SAODV in which H is the cost of performing Hash. About SAODV it can be explained that when the considered node itself is the source of a request or reply it does not pay for Hash. This means that its cost equal 2S where S is the cost of digital signature. On the other hand, if the node is not the source hashing cost is obtained by subtracting maximum distance step from current number of steps. Four overall states are generated for ARAN each of which has its specific costs. For instance, if a faraway node is considered, estimating costs if the current signature leads to S + 4S' and the total cost is computed by summing result of all states.

Data of the following table are studied to examine the two protocols in terms of time:

TABLE II
Estimated costs of ARAN and SAODV for different node numbers

N	ARAN	SAODV
10	696.0	123.0
20	1463.6	184.6
30	2255.2	241.8
50	3814.4	353.4
60	4593.8	409.5
70	5373.6	457.9
80	6269.6	493.6
100	7712.4	601.0

As can be seen SAODV always has less costs than its rival (ARAN). Interesting results are achieved through simulation performed to estimate costs of the two protocols. Figure 3 shows the results:

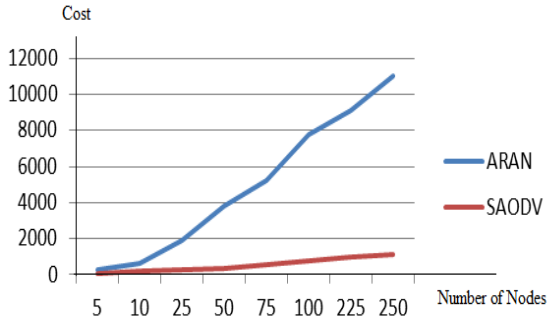

Fig. 3 comparing computational costs of ARAN and SAODV

In the figure above the horizontal axis represents number of used nodes and vertical axis shows costs. It is clear that computational costs of the two protocols are very different. SAODV is more optimal than ARAN respecting costs so that a 1:10 ratio is observed for huge number of nodes. An increase in node number better expresses the optimality. ARAN provides the secure route by ensuring identity, message integrity and unassailability through a certificate but it is too costly because of the need to certificate server and necessary investigation of middle nodes (for identification) besides increasing the volume of message being sent. On the other hand, having three main factors (Hash chain maker for hop-count, signer for identification and protocol implementation mechanism) SAODV imposes no burden on the message and has less delay [21]. Thus, it can be said that SAODV is faster than ARAN since it is less costly and it is more efficient in huge sensor networks such as thermal sensors in jungles. Lower costs reduce nodes' energy consumption, increase their life-span, optimize the exchanged burden and have many other advantages.

VI. CONCLUSION

Ad-hoc networks have big security weaknesses despite their suitable advantages and important applications and secure routing is one of the most considerable challenges facing them. Two main protocols of these networks, ARAN and SAODV, have also their own advantages and disadvantages. But the comparison presented in this paper showed that SAODV is more optimal than ARAN since it tries to reduce costs. The two protocols' cost difference is to the extent that a 1:10 ratio is observed for huge number of nodes and this where optimality of secure routing is considered. Lower costs of this protocol reduce nodes' energy consumption and impose fewer processes on them.

REFERENCES

[1] B. Awerbuch, A. Mishra. Introduction to Ad-hoc Networks. CS-647: Advanced Topics in Wireless Networks, Department of Computer Science, John Hupkins University.
[2] C. K. Toh Ad-hoc Wireless Networks: Chapter 3. Prentice Hall, 2002.
[3] Dr. M K Soni, Pr. P K Suri, P Tomar. A Comparative Study For Secure Routing In MANET. International Journal of Computer Applications(IJCA), 2010.
[4] K Sanzgiri, B.Dahill, B.N.Levine, C.Shields, E.M. Belding-Royer. a Secure Routing Protocols for Ad-hoc Networks. IEEE International Conference on Network Protocols (ICPN), 2002.
[5] L. Zho, Z. J. Haas. Securing Ad-hoc Networks. Microsoft Research. Cornell University, Ithaca, NY 18453, 1999.
[6] S. Capkun, L. Butty and J-P. Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. Laboratory for Computer Communications and Applications (LCA), School of Information and Communication Sciences (I&C) Swiss Federal Institute of Technology Lausanne (EPFL)CH-1015 Lausanne, Switzerland.
[7] D. Balfanz, D. K. Smetters, P. Stewart, and H. Chi Wong Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. Symposium on Network and Distributed Systems Security.
[8] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi. Secure Pebblenets. ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2001.
[9] S.-Ju Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia. A Performance Comparison of Ad-hoc Wireless Multicast Protocols. Wireless Adaptive Mobility Laboratory, Computer Science Department, University of California, Los Angeles, CA 90095-1596.
[10] C. de Morais Cordeiro, D. P. Agrawal. Mobile Ad-hoc Networking. OBR Research Center for Distributed and Mobile Computing, ECECS. University of Cincinnati, Cincinnati, OH 45211-0030-USA.
[11] Renuka A. , Dr.K.C.Shet. Hierarchical Approach for Key Management in Mobile Ad hoc Networks. International Journal of Computer Science and Information Security (IJCSIS), Vol. 5, No. 1, 2009.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

[12] J. Li, J. Jannotti, D.S.J De Couto, D.R. Karger, R.Morris. A Scalable Location Service for Geographic Ad Hoc Routing. MIT Laboratory for Computer Science.
[13] H. Li, Z. Chen, X. Qin. Secure Routing In Wired Networks And Wireless Ad Hoc Networks. Department of Computer Science , University of Kentucky, 2002.
[14] W. Zhang, R. Rao, G. Cao, G. Kesidis. Secure Routing In Ad Hoc Networks and a Related Intrusion Detection Problem. Department of Computer Science & Engineering, the Pennsylvania State University, University Park, PA 16802.
[15] G. Chockler, M. Demirbas, S. Gilbert, C. Newport, T. Nolte. Consensus and Collision Detectors in Wireless Ad Hoc Networks. MIT Computer Science and Artificial Intelligence Lab, Cambridge, MA 02139, USA, 2006.
[16] M. Nekovee, G. Freysson, A. Pace. Rumor-Based Broadcasting for Mobile Ad Hoc Networks. BT Research, Mobility Research Center, Adastral Park, Martlesham, Suffolk IP5 2EQ, UK.
[17] S. Mehla, B. Gupta, P. Nagrath. Analyzing Security of Authenticated Routing Protocol (ARAN). International Journal of Computer Science and Engineering (IJCSE), Vol. 02, No. 03, 2010, 664-668, 2010.
[18] D. Benneti, M. Merro, L. Vigano. Model Checking Ad hoc Network Routing Protocols: ARAN vs. endairA. Supported by the FP7-ICT-2007-1 Project No. 216471, AVANTSSAR. Dipartimento di Informatica, Universit` a degli Studi di Verona, Italy, 2007.
[19] M. Kumar Mishra. A Trustful Routing Protocol for Ad-hoc Network. Global Journal of Computer Science and Technology, Vol. 11, Issue 8, ISSN : 0975-4172 & Print ISSN : 0975-4350, 2011.
[20] S. Xu, Y. Mu, W. Susilo. Secure AODV Routing Protocol Using One-Time Signature. First International Conference on Mobile Ad hoc and Sensor Networks, Wuhan, China. Vol. 3794 , pp 288-297, 2005.
[21] D. Wadbude, V. Richariya. An Efficient Secure AODV Routing Protocol in MANET. International Journal of Engineering and Innovate Technology (IJEIT), Vol. 1, Issue 4, ISSN: 2277-3754, 2012.
[22] D. Lundberg. Ad hoc Protocols Evaluation and Experiences of Real Work Ad hoc Networking. Uppsala University, Department of Information Technology, SE-751 05 Uppsala, Sweden, 2005.
[23] T. Vinh Thong. Attacks Against Secure Routing Protocols. Budapest University of Technology And Economics, Department of Telecommunications, CrySyS Laboratory, 2011.
[24] J. C. Godskesen. Formal verification of the ARAN protocol using the applied pi-calculus. 6th International IFIP WG 1.7 Workshop on Issues in the Theory of Security(WITS'06), pages 99–113, 2006.
[25] A. Burak G. , M. Ufuc C. A Formal Security Analysis of Secure AODV (SAODV) using Model Checking. Turkish State Planning Organization (DPT) under the project number 2007K120610, 2007.
[26] S. Lu, L. Li, K.Y. Lam, L. Jia. SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack. International Conference on Computational Intelligence and Security (CIS 09), Pages 421-425, 2009.
[27] M. F. Juwad. Experimental Performance Comparisons between SAODV & AODV. Second Asia International Conference on Modeling & Simulation (AICMS 08), Pages 247-253, 2008.
[28] D. Cerri, A. Ghioni, P. di Milano. Securing AODV: the A-SAODV Secure Routing Prototype. Communications Magazine, IEEE, 2008.