Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

A Security Assessment Framework for Routing and Authentication Protocols of Mobile Ad-hoc Networks

Brijendra Kumar Joshi
Military College of Telecommunication Engineering, Mhow, India
Email: brijendrajoshi@yahoo.com
Megha Soni
Swami Vivekanand College of Engineering, Indore, India
Email: meghasoni@svceindore.ac.in

----------ABSTRACT----------

Security assessment of routing and authentication protocols is based on the comparison of basic and secured versions of protocols such as AODV, SAODV, DSDV, SEAD, ZRP, SRP, LHAP, HEAP etc. In this paper, a framework for security assessment is presented. It is a complete system that attempts to provide the promised services to each user or application. To assess the security of different protocols, a security index is assigned. The value of security index shows how much a protocol is secured. To assign the security index, security parameters have been found out and the performance of different protocols have been analyzed under normal condition, Black Hole attack, Wormhole attack, and DoS attack.

Keywords- **Routing; Authentication; Framework; Security Index; Performance Index**

Date of Submission: Jun 03, 2022 Date of Acceptance: Jul 09, 2022

1. INTRODUCTION

Early designers of protocols focused only on issues related to providing efficient communication paths within highly dynamic networks and disregarding importance of network security. As a result, Mobile Ad-hoc Networks (MANETs) are susceptible to attacks which threaten proper routing of messages within a network.

MANET security is very challenging and it is best attempted by taking into account the types of attacks which are possible and developing a comprehensive security analysis and solutions for secure transmission of information.

Network security demands features like Access Control, Integrity, Confidentiality and Authentication Support. Among these features, authentication is primary, as access or availabilities of all other services follow it. During authentication, validation and verification between the entities, prior to exchanging secret information, provides privacy protection.

2. SECURITY ANALYSIS OF BASIC ROUTING PROTOCOLS

The comparison is based on the basic protocol parameters suchas routing approach, loop freedom, routing metric, route recovery etc.

Table1. Basic routing protocols

Table 1 shows the comparative analysis of basic reactive, proactive and hybrid routing protocols [1].

Parameter	AODV	DSDV	ZRP
Routing Approach	On-demand	Table Driven	Hybrid
Loop Freedom	Yes	Yes	Yes
Routing Metric	Shortest path	Shortest path	Shortest path
Route Recovery	New route	Periodic	Start repair at failure point
Communication Overhead	High	High	Medium

2.1 Causes and Effects of Attacks on basic routing Protocols

Now let us consider the causes and effects of Black Hole, Gray Hole, Wormhole and (Denial of Service(DoS) attacks on the performance parameters of AODV protocol. The main causes of attacks on AODV are the following [2]-

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

- It is completely on-demand protocol.
- It uses message broadcasting process.
- It has flat routing.
- No mobility management.
- Uses shortest path algorithms.
- Does not have any process of authentication of non-mutable field.
- Only keeps track record of next hop.
- Real time attack is possible.
- No mechanism to observe the neighbor node activities.

Both Black Hole and Gray Hole attacks degrade the performance of AODV but the impact of Black Hole attack is more serious. AODV acts as a counter measure for Gray Hole attack and minimizes its effect and improves the reliability and effectiveness of the Ad-hoc network [2].

The communication overhead limitation in DSDV protocol makes attacker's efforts more communication efficient.

3. SECURITY ANALYSIS OF SECURE ROUTING PROTOCOLS

Secure routing protocols like Secure Ad-hoc On Demand Distance Vector Routing (SAODV), Secure Efficient Ad-hoc Distance Vector Routing (SEAD),Secure Routing Protocol (SRP) are compared in Table 2.

Table 2. Secure routing protocols

Parameters	SAODV	SEAD	SRP
Routing approach	On-demand	Table driven	On-demand
Loop freedom	√	√	√
Routing metric	Distance	Distance	Distance
Shortest path identification	×	×	×
Black Hole attack	×	×	×
Wormhole attack	×	×	×
DoS attack	×	√	√

Table 2 to highlight set of operational requirements and attack analysis.

In SAODV, use of digital signatures [3] prevents impersonation of source and destination nodes. It also uses the one way hash for hop authentication to prevent reduction of the hop count. But two malicious nodes can advertise that they have link between them and they can hold certain traffic in SAODV. It is also possible that intermediate node can corrupt the route discovery.On the other hand, use of public key cryptography imposes a high processing overhead.

SEAD is a robust routing protocol against multiple attackers. It uses efficient and inexpensive cryptographic primitives which play an important role in computation in bandwidth-constrained nodes.

As SEAD relies on doing neighbor authentication, it is unable to provide a way to prevent an attacker from tampering with "next hop" or "destination".

In case of SRP, route signaling cannot be spoofed. Alteration and fabrication of routing messages are not possible. And finally, malicious nodes cannot redirect routes from the real shortest paths.

On the basis of the various studied protocols a comparison of security against attacks is given in Table 2. It shows that a lot of work has been done for DoS attack but for Wormhole attack and Black Hole attack secure protocols are required.

4. SECURITYANALYSISOF AUTHENTICATION PROTOCOLS

Timed Efficient Stream Loss-Tolerant Authentication(TESLA), Light-Weight Hop-by-Hop Authentication Protocol (LHAP)and Lu and Pooch's algorithms are vulnerable to DoS attack [4]. LHAP is vulnerable to Wormhole and Man-in-the-Middle attack as periodic delayed key disclosure is not used in this algorithms (ReferTable 3).

Table 3. Attacks on authenticationProtocols

Protocol	Man in-the Middle Attack	Wormhole Attack	DoS Attack
Lu and Pooch's	×	×	√
TESLA	×	√	√
LHAP	√	√	√
HEAP	×	×	×

Hop-By-Hop Efficient Authentication Protocol(HEAP) offers some level of protection against insiders who forge packets and impersonate other insiders' nodes. HEAP successfully guards against many attacks by the outsider, such as DoS attack, Wormhole attack, Man-in-the-Middle attack, and flooding etc.

5. FRAMEWORK FOR SECURITY ASSESSMENT

A framework for security assessment is a complete system that attempts to provide the promised services to each user or application.

The key components of the framework are protocols, attacks, performance parameters, security parameters, *SI* and *PI etc.*

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

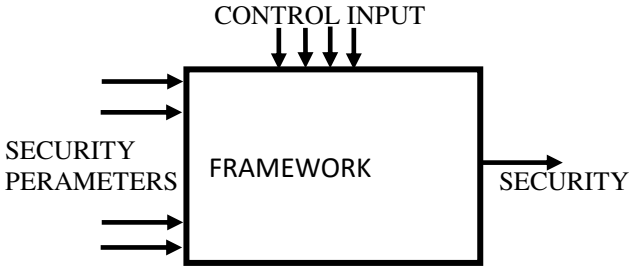

Fig. 1 Security assessment Framework

The objectives of designing the framework are the following:

- Security assessment of routing and authentication protocols.
- Performance analysis of routing and authentication protocols.
- To suggest the suitable routing and authentication protocol as per the user requirements.

In brief, the framework looks like a black box as shown in Fig. 1. The framework accepts the input values for different parameters and outputs a single value between 0 and 1. Here, the value 1 means the strongest system on which no attack can be launched. Obviously, we did not find any set of parameters for which this value could be achieved.The framework may be suitable for developing proposals for potentially new protocols for routing and authentication.

5.1 Control Input (CI) of Framework

The design parameters that serve the desired service to the user areProtocol Version(CI_1), Throughput (CI_2), PDR(CI_3), Delay(CI_4), Memory Overhead (CI_5), Routing Overhead(CI_6),Scalable(CI_7), CPU Time (CI_8).

5.2 Security parameters

Primary Security Parameter(PSP) andSecondary Security Parameter (SSP)are the security parameters of routing protocols. As a result of the study, it is found that the following are the PSPs:

5.2.1 Basic / Secure Version

A protocol may be basic protocol like AODV or secure version of the basic protocol like SAODV.

5.2.2 Routing approach

There are different routing approaches such as on-demand, table driven or both, used to implement protocols. These approaches play an important role in the security assessment of routing protocols (refer Table 1 and 2).

5.2.3 Effect of Attacks

PSPs can assess the security of any protocol by considering the effect of different attacks like Black Hole attack, Gray Hole attack,Wormhole attack, DoS attack and Man in-the Middle attack etc.

5.2.4 Security Schemes

Different security schemes such as Secret key,Message Authentication Code(MAC), Hash chain and Digital signature etc. are called SSPs. They are used to secure the basic protocols. These are the key parameters of security assessment.

5.3 Security parameters of Authentication protocol

When the authentication protocols were explored, it was found that the security of such protocols can be assessed with the help of following PSPs [5]-

- Effect of Attacks
- Source / Hop-by-Hop authentication.
- Application of MAC
- Trust bootstrapping
- Trust maintenance
- Use of Digital signature
- Delay time or varied delay in key disclosure

5.4 Protocol Index Value(PIV) of protocols

To assess the security in designed framework, the PIV shave been assigned forCI, PSPs and SSPs of each protocol. The assignment of values is based on the study of performance and behavior of different protocols [1], [4], [6-16].

5.4.1. *PIV for CI of routing protocol*

The range of $PIV$is different for different parameters. The range of PIV in the framework is $0 \leq PIV \leq 10$. The selection of "None" as an input, shows that no CI is applicablein assessment process. PIV can be assigned by the following relations:

$$\text{PIV} = \begin{cases} 0, \text{CI}_1 = \text{SP} \vee \text{AP} \\ 1, \quad \text{CI}_1 = \text{BP} \end{cases}$$

$$\text{PIV} = \begin{cases} 0\,, 0 < C1_2 \leq 20\% \\ 1, 20\% < C1_2 \leq 40\% \\ \quad . \\ \quad . \\ 5, 80\% < C1_2 \leq 100\% \end{cases}$$

$$PIV = \begin{cases} O, 0 < C1_3 \leq 20\,\% \\ 1, 20\,\% < C1_3 \leq 40\,\% \\ \quad . \\ \quad . \\ 5, 80\,\% < C1_3 \leq 100\,\% \end{cases}$$

$$PIV = \begin{cases} 1O, C1_4 \leq .001ms \\ 8, .001ms < C1_4 \leq .01ms \\ \quad . \\ \quad . \\ 2, 10ms < C1_4 \leq 100ms \end{cases}$$

$$PIV = \begin{cases} 1, C1_5 < .1 \\ 2, .5 < C1_5 \leq .75 \\ 1, C1_5 < .1 \end{cases}$$

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

$$PIV = \begin{cases} 3, 0 < C_6 \\ 2.25, 25\% < C1_6 \leq 50\% \\ 1.5, 75\% < C1_6 \leq 75\% \\ .75, 75\% < C1_6 \leq 100\% \end{cases}$$

$$PIV = \begin{cases} 1, C1_7 \leq 100 \\ 2, 100 < C1_7 \leq 100 \\ 3, 1000 < C1_7 \end{cases}$$

5.4.2. *PIV for* PSP *of routing protocol*

- If protocol version is secure, the assigned PIV is between 2 and 3 and for basic protocol it is 1.
- PIV is1, if routing approach is on- demand; for table driven and hybrid protocols, the assigned PIV is 2 and 3 respectively.
- PIV is assigned for each attack analysis. It is low if the severity of attack is high. If Black Hole attack, Gray Hole attack and Wormhole attack unable to degrade the performance of the protocol, the$PIV = 3$ else$PIV < 3$.

5.4.3. *PIV for SSP of routing protocol*

If any one of SSP- Secret key, MAC, Digital signature, Hash chain and Cryptography mechanism is used in the protocol, $PIV = 3$ else$PIV = 0$.

5.4.4. *PIV for PSP of authentication protocol*

- The assigned value of PIV is 1 for authentication protocol, as they are secure version.
- PIV is 1, if Man in-the Middle attack, Wormhole attack and DoS attack are unable to affect the performance of protocols.
- PIV is assigned for following PSP or security schemes separately. If Source / Hop by Hop authentication, MAC, Trust bootstrapping, Trust maintenance, Digital signature in trust management, Delay time / varied delay in key disclosure are applicable in protocol, $PIV =$ 1else$PIV = 0$.

5.5 Security Index(SI)andPerformance Index(PI)

SI of any protocol can be defined as the normalized value of the summation of the assigned PIV of security parameters.

The value of SI shows that how much a protocol is secure. A protocol is highly secure if SI is high (Refer Table 4). SI of routing and authentication protocols can be calculated by using the following formula.

$$I_{PSP} = \sum PIV\ of\ PSP \quad (1)$$

$$I_{SSP} = \sum PIV\ of\ SSP \quad (2)$$

$$SI = \frac{I_{PSP} + PIV\ of\ CI_1\ (I_{SSP})}{N} \quad (3)$$

Table4. Framework for SI of routing protocol

Where N is the sum of maximum PIV of SSP and PSP. It is 30 for routing protocol and 10 for authentication protocol.

Security Parameter	PIV of protocol					
	AODV	SAODV	DSDV	SEAD	ZRP	SRP
Secure	1	3	1	2	1	2
Routing approach	1	1	3	3	2	-
Black Hole attack	1	3	1	3	2	3
Wormhole attack	1	3	1	2	1	3
DoS attack	1	3	2	2	1.5	2
Secret key	0	3	0	3	0	3
MAC	0	0	0	0	0	3
Digital signature	0	3	0	0	0	0
Hash chain	0	3	0	3	0	0
SI	.16	.73	.26	.6	.25	.6

PI of any protocol can be defined as the normalized value of summation of assigned value of all CI.

$$PI = \frac{\sum PIV\ of\ CI}{n} \quad (4)$$

Where n is the sum of maximum PIV of all applicable CIs.The maximum value of n is 30.

PI is required either to find the suitable solution as per the user requirements or to analyze and compare the performance of protocols (Refer Table 5).

Table5. Framework for *PI* of routingProtocol

CI	PIV of protocol					
	AODV	SAODV	DSDV	SEAD	ZRP	SRP
CI_1	0	1	0	1	0	1
CI_2	2.5	2	4	3.5	3.5	3
CI_3	5	4.5	4	4.5	5	4.5
CI_4	3.5	1	10	8	10	9
CI_5	3	2.5	1	1.5	2	2.5
CI_6	2	1	1.5	1	3	2
CI_7	2	1.5	1	.5	3	2.5
CI_8	-	-	-	-	-	-
None	-	-	-	-	-	-
PI	.6	.45	.7	.67	.83	.81

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

SI and *PI* are independent of each other. A protocol which has high *PI* can perform better than others and also suitable for required service. *PI* can be calculated for minimum one *CI*. For no control input it is 0.

Table6. Framework for *SI* of authentication protocol

Security Parameter	*SI* value of protocol			
	LHAP	HEAP	TESLA	Lu and Pooch's
Secure	1	1	1	1
Man in-the Middle attack	0	1	1	1
Wormhole attack	0	1	0	1
Dos attack	0	1	1	0
Source / Hop by Hop authentication	1	1	0	1
MAC	0	1	1	1
Trust bootstrapping	1	1	1	1
Trust maintenance	1	1	0	1
Digital signature	1	1	0	0
Delay time / varied delay in key disclosure	0	0	1	1
SI	.5	.9	.6	.8

Table7. Framework for *PI* of authentica-tion protocol

Performance Parameter	*PI* value of protocol			
	LHAP	HEAP	TESLA	Lu and Pooch's
CI_1	1	1	1	1
CI_2	4	4	4	2
CI_3	2.5	2.5	2.5	1
CI_4	6	10	1	1
CI_5	1	3	.5	.5
CI_6	-	-	-	-
CI_7	2.5	.5	2.5	-
CI_8	2	3	1	1
None	-	-	-	-
Overall *PI*	.63	.8	.41	.2

6. RESULTS AND DISCUSSION

Table 4 and Table 5 show the *SI* and *PI* of different routing protocols for which the framework is designed. By comparing the *SI* of protocols it can be found that which protocol is more secured.

For example, if we assess the security of basic protocols such as AODV, DSDV and ZRP, it is found that DSDV is more secure than AODV. It is due to table driven routing approach of DSDV protocol.

ZRP offers almost same level of security as it uses both on demand and table driven routing approaches. On the other hand if we analyze the performance of these protocols, it is found that the overall *PI* value of ZRP is more than AODV and DSDV. But if we consider only one *CI* such as delay than the performance of DSDV protocol is much better than other basic protocols.

To assess the security of different secured routing protocols, the SI values were compared and are given in Table 4. It is found that SAODV is highly secured among all. It is due to the use of digital signatures in routing process. But it is not completely secured protocol.

The *PI* value of SAODV is very low as compared to SEAD and SRP. It is due to on demand routing approach. The overall performance of SRP is better than that of other given protocols as it is secured version of a hybrid protocol. But it is less secured than SAODV and SEAD protocol.

It is also found that the basic protocols have very low security index as compared to their secured versions. It is due to the application of different security schemes in secured routing.

The performance of HEAP, TESLA, LHAP and Lu and Pooch's algorithms were compared in Table 3 and it is found that TESLA is vulnerable to DoS attacks and thus it is important to secure time synchronization of all the nodes. Further, TESLA introduces very large latencies of several seconds making it unsuitable for real time applications.

LHAP is vulnerable to Wormhole and Man-in-the Middle attacks. Also, it needs very large memory at every node.

Lu's scheme suffers from overall poor performance as throughput and PDR are significantly low; though it has extremely low memory requirements.

HEAP is resistant to many outsider attacks such as DoS and Wormhole. It is suitable for use in MANETs for unicast, multicast or broadcast applications.

Table 6 and Table 7 show the *SI* and *PI* of different authentication protocols and it is found that HEAP

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

is highly secured and performs better as compared to other protocols which have been taken into consideration in the framework. It is due to the use of Hop by Hop authentication, digital signature, keys in trust bootstrapping and trust maintenance.

7. CONCLUSION

No protocol is able to cover all the threats and accomplish all security goals. This work also underscores the need for a more secured protocol that would deal with demanding requirements of MANETs.

First, most secured routing protocols have been designed by focusing on certain known attacks. Thus when an unknown attack may come up, one or more of these protocols may collapse.

Second, requirement of higher security demands more computational resources on each mobile node, something which is not easy to come by in a MANET environment. Therefore in MANETs, there always exists a tradeoff between higher security and higher performance.

Third, any security option is selected on the basis of what security aspects must prevail in a given operating environment; and in more ways than one these security options are not exclusive to one another.

Fourth, none of these provides complete security in MANETs operation. From the work emerges a table that demonstrates the fact that every secure protocol works within different limitations and to that extent provide security against limited threats.

A framework has been presented that assesses the security of routing and authentication protocols. The framework assigns a numerical value and suggests how much it is secured. In case of an unknown protocol, it suggests that which of the existing protocols the nearest one to satisfy the requirements.

REFERENCES

[1] A. Y. Zomaya, Algorithms and protocols for Wireless and Mobile Ad-hoc Networks: *A Taxonomy of Routing Protocols for Mobile Ad Hoc Networks,*(John Wiley Canada2009).

[2] M. Soni, and B. K. Joshi, Security Assessment of Routing Protocols in Mobile Ad-hoc Networks,*Proceeding of the International Conference on ICT in Business, Industry and Government,* Indore, India, 2016, 24

[3] M. Soni, and B. K. Joshi, Security Assessment of SAODV Protocols in Mobile Ad-hoc Networks.*Proceeding of the International Symposium Data Science and Big Data Analytics,* Indore, India, 2018, 347-355.

[4] R. Akbani,T. Korkmaz, and G.V.S. Raju, HEAP: Hop-by-hop Efficient Authentication Protocol for Mobile Ad-hoc Networks,*Proceedings of the Spring Simulation Multi conference,* Virginia, USA, 2007, 157-165.

[5] M. Soni, and B. K. Joshi, Security Assessment of Authentication Protocols inMobile Adhoc Networks, *International Journal of Computer Scence and. Information Security*,*19*(5), 2021, 36-40.

[6] S.Kaur, andA. Gupta, A Review On Different Secure Routing Protocols And Security Attacks In Mobile Ad Hoc Networks,*International Journal of Advance Engineering Technology5*(4), 2014,01-05.

[7] Argyroudis P. G. and O'Mahony D., Secure Routing For Mobile Ad Hoc Networks,*IEEE Journal on Communications Surveys & Tutorials,7*(3), 2005, 2-21.

[8] Shawkat, K. and Saaid G. O. S., Evaluating the performance of secure routing protocols in Mobile Ad-hoc Networks,*International Journal of Advanced Research in Computer and Communication Engineering, 1*(9), 2012, 710-716.

[9] A.Mohamed, Abdelshafy and P. J.B. King, AODV and SAODV under Attack Performance Comparison, *Proceeding of 13th International Conference on Ad-Hoc Networks and Wireless ADHOC-NOW*, Benidorm, Spain, 2014, 318-331

[10] P. Singh, N. Mann and T.G. Kaur, Study the impact of different attacks on Zone routing protocol in MANET. *International Journal of Modern Computer Science and Applications, 4*(3), 2016, 14-17.

[11] M. C.Trivedi, S. Yadav, and V. K. Singh, Securing ZRP Routing Protocol Against D DoS Attack in Mobile Ad Hoc Network,*Proceeding of International Conference on Data and Information Systems*, Singapore, 2019, 387-394.

[12] A. Saini and Anu, Analysis of Security Attacks and Solution on Routing Protocols in MANETs, *International Journalof Computer Science and Mobile Compting, 5*(6), 2016, 182-189.

[13] M. F. Juwad and H. S. Al- Raweshidy, Experimental Performance Comparisons between SAODV & AODV,*Proceeding of the 2nd Asia International Conference on Modeling & Simulation,*Kuala Lumpur, Malaysia, 2008, 247-252.

[14] S. M.Basha, S. R. Kumar, and R.V.Matam, Inclusive performance scrutiny of DSDV AODV and ZRP MANETs Routing Protocols, *International Journal of Advanced Computer Technology, 2*(5), 2014, 31-42.

Volume: 14 Issue: 01 Pages: 5287-5293(2022) ISSN: 0975-0290

[15] Ashwin Perti, Evaluate Dynamic Source Routing ProtocolPerformance in Wireless MANET,*Int. J. Advanced Networking and Applications, 5*(5) , 2016, 2056-2059.

[16] Nitish Balachandran,Surveying Solutions to Securing On-Demand Routing Protocols in MANETs, *Int. J. Advanced Networking and Applications, 4*(1), 2012, 1486-1491

AUTHORS PROFILE

Dr. Brijendra Kumar Joshi is a Professor of Electronics & Telecommunication and Computer Engineering at Military College of Telecommunication Engineering, MHOW (MP), India. He has obtained BE in Electronics and Telecommunication Engineering from Govt. Engg. College, Jabalpur; ME in Computer Science and Engineering from IISc, Banglore, PhD in Electronics and Telecommunication Engineering from Rani Durgavati University, Jabalpur, and M.Tech. in Digital Communication from MANIT, Bhopal. He has more than 38 years of teaching experience. His research interests are programming languages, compiler design, digital communications, mobile ad-hoc and wireless sensor networks, image processing, software engineering and formal methods. He has number of research publications to his credit. He has supervised 12 Ph D thesis and currently supervising two research scholars. He has authored two books on Data Structures and Algorithms in C/C++ published by Tata McGraw-Hill, New Delhi.

Megha Soni Ph.D.in Electronics and Telecommunication Engineering from MCTE, Mhow, DAVV University Indore, India. She has obtained BE in Electronics and Telecommunication Engineering from Govt. Engg College, Sagar; M.E in Digital Communication from Davi Ahilya University Indore. She joined as an Assistant Professor in Electronics & Communication in Dec. 2005. Her research interest is in security assessment of routing and authentication protocols of Mobile Ad- hoc Networks.