Path Authentication in Heterogeneous MANET using Extended Route Authentication Protocol (ERAP)

Rekha B, D V Ashoka

***Abstract*— Inter-domain routing and its dynamic nature imposes many challenges in the field of heterogeneous Mobile Adhoc networks. Inter-domain path authentication of the intermediate relay nodes can be affected by nodes' selfishness and many constraints introduced by heterogeneous MANET. This situation brings severe security threats. This paper introduces an Extended Route Authentication Protocol (ERAP) which uses a probabilistic route authentication mechanism to ensure reliable data packet transmission between intermediate nodes of a heterogeneous mobile Ad-hoc network. The proposed method provides flexibility in correct forwarding behaviours of nodes. It also ensures an effectiveness against malicious and selfish behaviour of some intermediate nodes. This study illustrates a mathematical analysis of the proposed system with respect to various parameters where IDRM and AODV have been considered for the demonstration of performance metrics.**

***Index Terms*— Composite MAC, Inter-domain Route Authentication, Mobile Adhoc Network.**

I. INTRODUCTION

All the nodes in mobile adhoc network (MANET) are routers by themselves. The mobile adhoc network consists of multiple nodes in random mobility condition and completely decentralized in nature. The areas of MANETs have been shrouded by multiple problems ranges from intermittent link breakage, energy consumption, routing, Quality-of-Service, and security. This paper essentially discusses about the issues of security. Addressing the security issues in MANETs is quite a challenging problem owing to the decentralized nature of the network [1]. MANET is already inflicted with various forms of lethal attacks e.g. denial of service, sybil attack, blackhole attack, flooding attack, sinkhole attack, replay attack, flooding attack, wormhole attack, rushing attack, etc. [2][3][4][5]. In past decades, there have been various forms of discussion about the security solutions towards the existing adversarial threats. However, the extent of work being done towards wormhole attack in mobile adhoc network is quite less. Basically, in wormhole attack, the adversary compromises minimum two nodes in order to create a tunnel [6]. The adversarial node considers the tunnel to route the data packets. The channel capacity of the tunnel is increased by the adversary in order to increase the traffic rate to be incoming on the tunnel in the peak traffic condition. Owing to large availability of bandwidth, the rate of data transmission is quite high in the tunnel. Implications of the wormhole attacks will lead to disruption of the routing data. Owing to the tunnel formation, it will lead to disclosure of other adversarial attacks e.g. black whole attack, Sybil attack, DoS etc. Wormhole attack will also lead to intrusively gain an access to confidential and sensitive data. It will also affect the surveillance system outcomes and lead to declination of services running over physical layers [7] [8] [9]. From past decades there has been a stream of research work towards security issues in MANETs. But before starting discussion about security, it is also essential to study the algorithm compatibility. A security algorithm usually runs on mobile nodes, but it is the routing protocol that mainly governs the communication requirements. A mobile node in this concept can be a cellular phone, laptop, Smartphone, or any other mobile device where the hardware configurations highly differ. All these devices perform well and optimal with availability of sufficient battery lifetime and starts degrading if the energy of the devices starts dissipating much. Another reality in the viewpoint of cryptography is that security algorithms have a complex encryption scheme, which consume maximum of residual energy of the mobile nodes. Hence, the existing cryptographic-based approach may provide 100% robust encryption scheme but that will not work out with wormhole attack. Because in such forms of attack, the traffic by itself gets directed to the tunnel in order to avoid congestion and thereby falls in prey of malicious programs. Moreover, another troublesome part of the wormhole attack is that incase the security solution is presented in the forms of intrusion detection and prevention system, than it will fail the authentication system. In such condition the identified node will be the compromised regular node and no possibility of exploring the adversarial node IP. This paper presents a novel routing procedure that supports any future cryptographic protocol in terms of energy efficiency as well as communication performance. It is also resilient against wormhole attack equally. Section II discusses about existing literatures followed by issues in Section III. Proposed system is discussed in Section IV followed by Implementation techniques in Section V. Result discussion is done in Section VI, while the summary of the paper is carried out in Section VII.

II. RELATED WORK

This section discusses about the existing research work and the problems associated with it.

A. Existing Literatures

The study of Nazeeruddin et al [10] introduced a distributed agent based dynamic host auto configuration protocol for heterogeneous MANET nodes. The proposed method uses a disjoint set of IP addresses. The comparative

Rekha B, Research Scholar in department of CSE, Jain University, Bangalore. She received her M.Tech in Computer Networking and Engineering from VTU.

Dr. D.V Ashoka, Professor working in Computer Science and Engineering Department, JSSATE, Bangalore. He received his M.Tech in Computer Science and Engineering from VTU, Ph.D degree in Computer Science from Dr. MGR, University, Chennai.

analysis of the proposed scheme indicates its robustness and efficiency as compare to other existing traditional schemes. An efficient and novel Inter-MANET routing protocol has been proposed by Lee et al [11] which can be applicable for handling the heterogeneity and dynamicity of the mobile Adhoc networks. The experimental outcomes of the proposed system highlights that it can transparently adapt with the topological changes of the MANET. The study also represented the scalability of the proposed system. Shulman and Waidner [12] proposed a method which has been named as Domain Name system security extensions (DNSSEC) which is considered as a very efficient method in the field of cyber forensics. The authors also reviewed the proposed system in terms of DNS cache poisoning. Waheed and Karibsappa [13] presented the mathematical modelling for a new routing technique which has been named as QoS routing protocol for heterogeneous mobile Adhoc networks. The proposed techniques reduce the number of routing hops and also optimize the computational overhead. A study proposed by Jaroodi [14] investigated and analyzed various security issues associated with common types of MANET. The proposed study also detected various specific requirements for secure and reliable data transmission. A secure and spontaneous ad-hoc network based on direct peer to peer iteration protocol for giving users secure network connectivity has been developed by Lacuesta et al. [15]. The proposed system has been developed with an objective of improving the communication and data transmission in between nodes with less resource.

Kaur [16] considered a single hop cluster ad-hoc network and also LEECH for performing a comparative analysis of various homogeneous and heterogeneous protocols of Mobile Adhoc networks. A novel hierarchical anonymous on demand routing protocol has been developed in the study of Liu et al [17] which can control the overhead incurred by existing flat anonymous routing protocols. Konate and Gaye [18] proposed a secure algorithm which uses the concept of reputation. The study also introduced an analytical model which can be useful for the future research direction of secure and reliable communication associated with MANETs. A study carried out by Gunasekaran and Premalatha [19] has introduced a secure privacy-preserving architecture in wireless mobile Adhoc networks for the mitigation of various routing attacks performed by many adversaries. The experimental analysis and results prove the effectiveness of the proposed system with respect to privacy and security in heterogeneous MANET environments. Gong et al [20] discussed various security problems of heterogeneous MANET environments. In the paper a threat model for collaborative attacks has been developed for scrutinizing the vulnerabilities of real heterogeneous MANET. The study of Yi and Kravets [21] has been developed a key management technique for heterogeneous infrastructure of MANET.

B. *Problem Identification*

Presence of so many heterogeneous nodes in a heterogeneous MANET increases the probability of various malicious attacks thus the delay and throughput associated with the data packet transmission will increase. Various security flaws associated with the Mobile Adhoc network also affects the quality of services (QoS) and the security credentials of the whole mobile Adhoc network systems. There many existing techniques which impose various limitations such as expansion of system through put and reduce the delay of the network by choosing a shortest route from the base station to the selected cluster head. The cluster heads also maintain a table where information associated with the nodes which are having the best delay to the destination node is maintained. As in the heterogeneous mobile Adhoc network various types of mobile nodes can be present and also many nodes join and leave at the same time thus there should be some mechanism for maintain and updating tables for so many intermediate nodes exchanging their data packets. There are many methods which do not talk about any type of inducements associated with data packets forwarding. Those techniques also include some of the methods which reduce the battery consumption of the mobile nodes while forwarding information or data packets to the other user.

The formation of a cluster in a Mobile Adhoc network enables the processing of selecting cluster heads as Adhoc network nodes can leave and join a particular domain anytime. So that a lot of power consumption will happen due to the updating of sent data packets and received data packets. As lot of nodes can be connected to a Mobile Adhoc network thus it will increase the computational complexity and the response time for two way communications will be much higher. A close comparative analysis in the field of various heterogeneous wireless networks protocols such as Unified Cellular ad hoc Network (UCAN), (Integrated Cellular Ad hoc Relay (iCAR), and Scalable Proxy Routing (SPR) shows that these protocols are not efficient due to very poor security mechanisms which have been installed at all. These all protocols consider a combine network scenario of a cellular network and a mobile Adhoc network, where the shortest route from source node to destination node is selected by the cluster head. The authors have not mentioned any efficient mechanism for if a node of a particular route get malicious and have the smallest delay to the destination node in that case the node will be considered as a cluster leaded or not. Although a node is selected as a cluster head, it will forward the error-based information with its neighbors. As a result the malicious node can damage the whole system performance by sharing the wrong information. And the mentioned protocols for heterogeneous MANETs are susceptible to various kinds of attacks such as wormhole, Sybil and black hole attacks. Those methods do not have any effectiveness for removing the security threats from a node connected to heterogeneous MANET.

III. PROPOSED SYSTEM

In this paper a novel approach which is named as Extended Route Authentication Protocol (ERAP) has been proposed. As in the recent times inter-domain route authentication between source nodes and the destination nodes for heterogeneous MANET has become very challenging due security issues so that the proposed system gives a very efficient and secure data transmission over a heterogeneous mobile ad-hoc network. The concept of the proposed system shows that it utilizes composite MACs for different types of authentication whereas it uses some of the algorithmic processes for computing the path authentication module. The proposed technique also uses a shared key the data packet bits and a flag value for inter route authentication which will be executed between various computing devices of a heterogeneousMANET. The following figure 1 represents an overview of the proposed system.

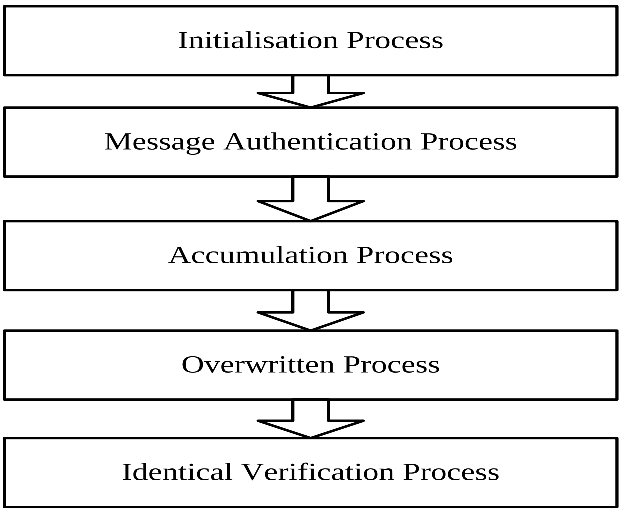

Figure 1 Proposed System

The proposed algorithm also signifies the robustness and it also reduces the computational complexities and probability associated with complex trade-offs for secure data transmission. It uses a secret shared key between source and destination nodes. It computes a FLAG value with respect to the data aggregation and authentication of Mac. Every node uses privately shared secret key with its neighbor node while transmitting data packets. The destination nodes verify the key and validate the received message and acknowledge the sender node. Various mathematical equations and algorithmic steps associated this proposed Extended Route Authentication Protocol for heterogeneous MANET has been illustrated in Section IV. The proposed architecture also validates various routing schemes in between heterogeneous nodes with respect to message and the Flag value attached with the data packets. The proposed system also ensures the security aspects and uses packet IDs for detecting behavior of selfish and byzantine adversaries. It verifies the authenticated Flag Values by backtracing and also validates routes with higher probability.

IV. IMPLEMENTATION TECHNIQUE

This section introduces an Extended Route Authentication Protocol (ERAP) for MAC layer which utilizes the concept of composite MACs rather than aggregate MACs. The proposed system makes full use of the properties associated with data aggregation. It is also noticed that optimizing the MAC layer tag size to a small number such as 4 to 8 can affect the authenticity of the MAC layer protocols. It yields some probabilistic results and indicates vary less authenticity. The proposed system analyzes various transmitted data packets in terms of per packet where the it yields packet loss with respect to the arrival packets at a particular node. The proposed technique uses composite MAC system as it can be very useful for reliable, authentic communication associated with MANET. It controls the route cost trade-offs which are very necessary for data transmission and communication over a huge network like MANET. The Algorithm takes a key which is denoted by $AK_{s,d}$ where the authentication key works between source node s and destination node d. The sender set the flag value with respect to the Mac authentication tag and shared keys between the sender and the receiver. The sender then transmits the data packets along with flag value. The next two steps of the proposed algorithm represent aggregation and authentication of the MAC whereas on input a node S shares its Flag value and data packets with its destination node. It computes another flag value which takes value of XOR operation that has been performed between previous flag and the Mac value. The verification step introduces how the destination node D authenticates and verifies flag values which comes from the source node as input along with the data packets and an expected set of values which is denoted by *L*. The calculated aggregated Mac can be utilized in order to compute the sequential collective MAC. In the process of composite MAC the sender node transmits the data packet along with the shared key and the actual message as an input. The sender node also computes the flag value with the use of composition operator which combines the aggregation of Mac and Flag values , where the Mac contains the message bits and the secret shared key $SK_{m,n}$. This process also signifies three different types of sub processes which are Aggregate, Overwrite, Keep Identical methods.

1. *Accumulation Process:* This is regarding calculating a composition logical operation between the flag value of the sender node data packets with the secret keys. Mathematical modelling for the Accumulation process is highlighted below.

$$\text{Flag} \circ \text{MAC}_{SK_{m,n}}(\text{m}) == \text{Flag} \otimes \text{MAC}_{SK_{m,n}}(\text{m}) \quad (1)$$

2. *Overwritten Process:* This performs a composition operation between the flag values and the MAC authentication security keys. The following equation shows a theoretical of overview of the proposed method.

$$\text{Flag} \circ \text{MAC}_{SK_{m,b}}(\text{m}) == \text{MAC}_{SK_{m,n}}(\text{m}) \quad (2)$$

3. *Identical Verification Process:* The last step which is termed as identical verification state has been highlighted below. This step computes the flag value of the sent message and it also uses an expected ordered set I where the number of nodes N ∈ I. Equations (3) and (4) represent the mathematical modeling of these steps.

$$\text{Flag} \circ \text{MAC}_{SK_{m,n}}(\text{m}) == \text{Flag Value} \quad (3)$$

$$\text{FLAG} == \in \circ \text{MAC}_{SK_{m,n}}(\text{M}) \quad (4)$$

V. RESULT DISCUSSION

This section introduces the result discussion of mathematical and theoretical analysis of the proposed Extended Route Authentication Protocol (ERAP) where as a method of back tracing has also been introduced. The proposed method also utilizes the enhancement of composite MAC. Suppose a set of node Z which can possibly modify the authentication flag but in the worst case all the nodes belong to a coalition network N. The backtracking computes the authentication tags with respect to all possible combinations of MACs. The best possible combination of Macs will be $2^{|z|}$. The mathematical analysis associated with the proposed system shows that the worst complexity of back tracing will be $O\left(2^{|z|}\right)$. There are some constraints which affect the backtracking so that the proposed model limits the range of the backtracking within a limited depth which is considered as L << $|Z|$. It is also found that optimizing the computational complexities decreases the ability for producing the desired result of backtracking. The theoretical approach also highlights that the worst case complexity of the backtracking can be exponential with respect to various sub flags whereas the respective Mac ID of length L is divided and segmented into S_n. Equation (6) defines the Mathematical modelling for this step which is defined below.

$$\mathrm{MAC}_{i,d} == \mathrm{MAC}_{i,d-1}\left|MAC_{i,d-2}\right| \ldots\ldots\ldots \left|MAC_{i,d-S_n}\right| \quad (5)$$

The above equation performs the concatenation operation of MACs flags with respect to the normal tags of full length. The analysis also clarifies that if a Flag value is segmented into 4 sub flags then the mathematical analysis and interpretation will intensifies by a factor of 4. There are some constraints which create some drawbacks in the case of back traceable flags which are the smaller probabilities. The second mathematical analysis includes the pseudo random selection of a small subset of nodes. This ensures the authentication scheme and aggregation of nodes on a per packet basis. The proposed scheme also ensures that the choice of node for aggregation, overwrite and keep undistinguishable will be updated to its respective neighbor nodes and the destination node. F and G are considered as aggregated and modified sub flags that computes the aggregation. 1-F-G represents the fraction of sub-flags which care considered as identical and indistinguishable by the node. The following equation shows how node m considers nth sub flag value in order to aggregate MACs of its data packets. The equation also uses a publicly Pseudo random function (PRF). The pseudo random function uses a packet ID, shared key and a jth sub flag for computing the parameters F and G. the equation for this theoretical overview is given below.

$$\text{PRF (P-ID, Key, Tag)} \leq \text{Packet Size. } 10^{\gamma}\text{. MOD } 10^{\gamma} \quad (6)$$

The process also executes the inter domain route authentication which is explained in the equation (8)

$$\text{P. } 10^{\gamma} < \text{PRF (P-ID, Key, Tag)} < \text{M + N. } 10^{\gamma} \text{ mod } 10^{\gamma} \quad (7)$$

The proposed ERAP method also keeps the pseudorandom function identical whereas $\mathrm{SK}_{m,n}$ is the privately shared key between the node m and the node n. The proposed algorithm also computes the probability associated with the accuracy of packet ID where Packet ID $\in [0, 1]$. This also ensures the authenticity of the transmitted data packets with respect to the packet identifiers. This process also initialize that the Packet ID can be any sequence of the data packet which also considered as sequence number. The packet IDs also ensure the choice of compositions which varies randomly on a per packet scheme. A comparative overhead analysis with respect to various parameters of reactive and proactive routing protocols have been highlighted in Table-1 where the proposed study compares the performance metrics of the proposed algorithm with two other algorithms which are Inter Domain Routing Protocol (IDRM) and AODV respectively.

Table 1 Comprehensive Analysis

Nodes	Factors	Proposed	IDRM	AODV
20	Delay (Sec)	0.00023	0.00141	0.00784
	Execution Time (Sec)	0.00145	0.00234	0.00543
	Network Load (Bits/Sec)	98,967	187,261	186,287
40	Delay (Sec)	0.01234	0.01528	0.04181
	Execution Time (Sec)	0.00123	0.00278	0.01256
	Network Load (Bits/Sec)	187,567	368,120	456,345
80	Delay (Sec)	0.01546	0.01789	0.16789
	Execution Time (Sec)	0.00567	0.00345	0.06789
	Network Load (Bits/Sec)	436,798	662,275	704,935

The computational efficiency as compared to the proposed Extended Route authentication Protocol has been highlighted in the above table. It shows that the Execution time, Delay, and Network load are very less as compare to others. The proposed protocol also ensures the reliable 2-way communication for heterogeneous mobile nodes.

VI. CONCLUSION

This paper introduces a novel Extended Route Authentication Protocol (ERAP) which utilized the concept of a novel probabilistic route authentication mechanism for inter-domain MACs. It also identifies the presence or absence of incorrect data packet forwarding behavior associated with the heterogeneous nodes of MANET. It computes a length of 4 or 8 bits signature of the authentication flags. It also ensures high efficiency in terms of time and space complexity. The comparative analysis which is highlighted in the Table-2 shows that the proposed algorithm is very efficient as compare to existing routing techniques such as Inter Domain Routing Protocol for MANET (IDRM) and AODV. The mathematical modelling represented in section III and IV also make sure that the proposed system can be applicable in informal security analysis of MANET. It can designate so many techniques for authenticate routes with higher probability effectiveness.

REFERENCES

[1] S. Jacobs, “Engineering Information Security: The Application of Systems”, *Engineering Concepts to Achieve Information Assurance, John Wiley & Sons*, 2011

[2] J. L._Mauri, S.M. Thampi, D.B. Rawat, “Security in Computing and Communications”, *Springer*, 2014

[3] D.B. Rawat, “Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications”, *IGI Global*, 2013

[4] S. C. Satapathy, P. S. Avadhani, S. K. Udgata, S. Lakshminarayana, “ICT and Critical Infrastructure”, *Springer- Proceedings of the 48th Annual Convention of Computer Society of India*, 2013

[5] S. Khan, J. L. Mauri, “Security for Multihop Wireless Networks”, *CRC Press*, 2014

[6] B. Issac, N. Israr, “Case Studies in Secure Computing: Achievements and Trends”, *CRC Press*, 2014

[7] M. Ali, “Mitigation of Passive Wormhole Attack in Wireless Sensor Network”, *Lap Lambert Academic Publishing*, 2015

[8] A. Zade, “A New Cluster Approach for Wormhole Attack Removal in MANET Using NS2: A New Approach for Wormhole Removal and AODV Evaluation Using NS2 Simulation”, *Lap Lambert Academic Publishing*, 2012

[9] L. Buttyán, J-P Hubaux, “Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing”, *Cambridge University Press*, 2007

[10] M. Nazeeruddin, G. Parr, and B. Scotney, “Fault-tolerant dynamic host auto-configuration protocol for heterogeneous MANETs",pp .19-23,2005.

[11] S.H. Lee, S.HY.Wong, C.Chau, K.Lee, J.Crowcroft, and M.Gerla. "InterMR: Inter-MANET routing in heterogeneous MANETs", pp. 372-381, 2010

[12] H. Shulman, and M.Waidner, "DNSSEC for cyber forensics", Vol.1, pp.1-14,2014

[13] M.A. Waheed, and K.Karibasappa, "QoS Routing for Heterogeneous Mobile Ad Hoc Networks", 2008.

[14] A-Jaroodi, Jameela, "Routing Security in Open/Dynamic Mobile Ad Hoc Networks", vol.4, pp.17-25,2007

[15] R. Lacuesta, J. Lloret, M.Garcia, and L.Peñalver, "A spontaneous ad hoc network to share WWW access", 2010.

[16] M. Kaur, "Comparative Study of Homogenous and Heterogeneous Mobile Device Adhoc Networks", Retrived, 22nd , 2015

[17] J. Liu, X. Hong, J.Kong, Q.Zheng, N.Hu, and P.G.Bradford, "A hierarchical anonymous routing scheme for mobile ad-hoc networks", pp. 1-7, IEEE, 2006

[18] K. Konate, and G. A. Y. E. Abdourahime. "Implementation and Test of A Secure Mechanism’s Modules in Routing Protocol of Manets with the theory of games",vol. 4,2012.

[19] M. Gunasekaran, and K.Premalatha, "SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks", vol.1, pp.1-12, 2013.

[20] T. Gong, B.Bhargava, J.Zhou, M.Azarmi, and C.Du, "Minimizing collaborative attacks in a real heterogeneous mobile ad hoc network using cooperative immunization model", Retrived, 21st August, 2015

[21] S. Yi, and R.Kravets, "Key management for heterogeneous ad hoc wireless networks", *IEEE*, pp. 202-203, 2002

BIBILIOGRAPHY

Rekha B is a Research Scholar in department of CSE, Jain University, Bangalore. She received her M.Tech in Computer Networking and Engineering from VTU. She has 15 years of academic teaching experience and 3 years of research experience. Her fields of interest are Ad-hoc Networks and Wireless Communications

Dr. D.V Ashoka, is a Professor working in Computer Science and Engineering Department, JSSATE, Bangalore. He received his M.Tech in Computer Science and Engineering from VTU, Ph.D degree in Computer Science from Dr. MGR, University, Chennai. He has 20 years of academic teaching and research experience. His fields of interest are Requirement Engineering, Operating System, Computer Organization, Software Architecture, Computer Networks and Cloud Computing.