Role of Cryptographic algorithms in Mobile Ad Hoc Network Security: An Elucidation

Veerpal Kaur, Kamali Gupta, Vidhu Baggan, Gagandeep Kaur, Amanjyoti

Abstract*: Mobile Ad hoc Network, an infrastructure-less network is emerging as one of the major dynamic areas of communication. Due to the rapid increase in the moveable devices, an appreciable growth in wireless network is witnessed in the recent years. As the network is growing, the number of intruders is also rising to find a loophole in the security of network to achieve their evil means. So the network is prone to a large amount of attacks like wormhole attack, black hole attack, malicious node attack etc. In order to alleviate such attacks, security measures should be strong enough to combat. The objective of this paper is to study the cryptographic techniques implemented on Mobile Ad hoc Network in order to provide security to the foundation-less systems. Year-wise distribution of the cryptographic approach implementation has been presented and analysis has been made in terms of existing implementation and future work that necessitates its efficacious implementation.

Keywords*: Mobile Ad Hoc Network, Cryptographic Techniques, Proactive techniques, Reactive techniques, Preventive techniques, Attacks.

I. INTRODUCTION

The society is moving at an alarming pace from wired world to remote correspondences. As the technology is rising, the need of portable systems has also been raising due to its mobility features. Remote systems which are portable can be categorized into two divisions: foundation and foundationless systems. Foundation systems have fixed pre-located cell sites and stations, on the other side, foundationless systems have no base stations and deployment is rapid [1].

Mobile Ad-Hoc Network usually called MANET is the fastest growing network in such category of networks. MANET comprises of nodes scattered at different geographical locations, connected among each other by a network of routers [2]. The routers rely on routing protocols which further rely on the routing tables in which most of the crucial information like node's IP or MAC addresses has to be saved for routing purpose. The security [3] of information at routing protocol level is also an important paradigm which cannot be ignored to achieve optimum security of MANET.

The need of cryptographic algorithms arises with a network that is vulnerable to attacks at various levels of security [4]. Some of the possible attacks are on nodes, routing protocols, the data transferred and the acknowledgement transferred. MANET suffers most commonly from wormhole, black-hole and gray-hole attacks. Cryptographic algorithms [5] such as RSA, AES, and hashing algorithms are well known for their durability and avoidance of such attacks.

The proposals from past, had made use of various cryptographic algorithms in order to eradicate the illegitimate use of the network resources. In nutshell, the article highlights about various factors and techniques involved in safeguarding the foundationless systems which is the prior need of the information technology world.

The organization of this paper inculcates a brief review of literature in section 2, comparative analysis of various techniques used in research are discussed in section 3 and conclusion in section 4.

II. RELATED WORK

A number of proposals have been made in the field of MANET to combat the risk to its security paradigms. Considering the major perspectives like security at node and protocol level have been achieved successfully. The section liberates existing researches done in the domain of MANET Security using cryptographic approaches.

With reference to [6], M. Razi and J. Quamar have discussed a seniority based trust model and PGP type certification service. The proposed methodology has worked primarily on key management and data security parameters. Secure routing protocols and IDS were not discussed in this paper. In the year 2010 [7], a technique called Most Balancing Credit Conserving (MBCC) key generation policies have been discussed which focuses on Key Management and Node Security issues of MANET. The presented work had no description of secure routing and Intrusion detection. The study of year 2012 is mostly focused on the dynamic behavior of MANET and evolution of key mechanisms has been taken place to secure such dynamic network [8]. Key management system using cluster based group multicasting technique came into existence. The scenario of MANET security changed when an efficient routing protocol called ALERT (An Anonymous Location-Based Efficient Routing Protocol) has been established to safeguard the communication ends [9]. A major transformation to the perspective of MANET security has been drawn when the solution providers' collaborated cryptographic algorithms in the security of acknowledgements transferred through the network and named the Intrusion Detection system as EAACK (Enhanced Adaptive Acknowledgement) by applying Elliptic Curve Cryptography with Dual-RSA and MD-5. The proposed system withstands Intrusion Detection, packet security and routing protocol security.

Revised Version Manuscript Received on 16 September, 2019.
***** Correspondence Author
Veerpal Kaur1, Kamali Gupta2, Vidhu Baggan3, Gagandeep Kaur4, Amanjyoti5
12345Chitkara University Institute of Engineering and Technology
Chitkara University, Punjab, India

The system has an assumption of fully trusting the nodes in the communication channel [10].

The security has been provided to packets, routing protocols but still the network needed strong mechanisms to detect the malicious behavior. An instant key generation mechanism to enhance MANET security has been put forwarded which concentrate on security of data packets, communicating devices along with detection of malicious behavior in the network [11]. The research work conducted in [12] and [13] focus has been kept on the key management schemes so as to reduce the risk of attacks and provided the countermeasures to save energy consumption of the end devices.

The need of key management along with strong cryptographic algorithms has risen in the year 2014 when the solution providers have options like AES and RSA to be used to secure data transfer. The research work liberated in [14] has collaborated RSA, AES and a hashing technique called MD-5. The resultant cryptosystem has been providing security on data transfer, routing and communication devices. Intrusion detection and packet delivery ratio have also been discussed.

The year 2014-2015 have seen vast advancements in adopting techniques like Intrusion detection with extended EAACK using one-hop ACK [15], which optimized the security of data, nodes and shared key, [16] has extended the findings of [15] by including RSA and DSA in the intrusion detection. The proposed IDS have key management mechanism and better packet delivery ratio.

Another technique yet came up with new way of Intrusion detection using EAACK has been seen in [17] which has made use of elliptic curve cryptographic algorithm which enhanced the packet delivery ratio and node security of the network.

A new approach called Hybrid Symmetric Cryptographic Technique using AES and MD-5 has been proposed in [18] which focused mainly on the detection and removal of malicious attacks on communicating devices and packets transferred.

As symmetric cryptographic approaches have many drawbacks [5] such as possible attacks and key security, a hybrid of RSA, AES and DES has been implemented on AODV routing protocol of MANET [19] to achieve routing security with key management and packet security. This paper has undoubtedly provided packet security, routing protocol security along with key management but lagged behind in packet delivery ratio and node security like challenges were not discussed.

Various methodologies had been proposed which made use of hybrid cryptography but there was a need to provide more security because no such algorithm except AES and RSA withstand the attacks fully. Therefore, paper [20] had been published which was based on security of data achieved using AES, MD-5 and digital signature using RSA. The end nodes, packets and shared key have been secured. Quite a similar approach had been implemented in [21] which enhanced the security of AODV protocol using DES and RSA.

In reference to [15-17], intrusion detection system [22], had been further improved using AES and RSA. This technique had improved the packet delivery ratio providing optimum security to the packets transferred.

The findings of [15-17] and [22] had further been improved by the intrusion detection approach called EAACK with AES, RSA and DSA [23] resulting in securing packets, routing protocols and keys. Another approach [24] for securing MANET using RSA, AES and SHA-256 along with EAACK had been proposed which has provided security to the nodes, routing protocols and packets transferred.

Intrusion detection and its proper functioning had been the main focus keeping in view the other parameters like node security, key management and secured data transferred through the network. A similar work had been proposed in the series by [25] which used RSA algorithm to secure the Intrusion Detection System in MANET.

Next section discusses about comparative analysis of MANET Security.

III. COMPARATIVE ANALYSIS OF MANET SECURITY

The research conducted in this article spotlight upon important developments taking place recently in the domain of MANET security. The study explicates three important parameters of security, mainly, preventive, proactive and reactive.

Preventive techniques are those techniques that work upon the key management involved in the network which is a crucial part of security. The key here can be a secret code which is known only to the sender and the receiver of the information. This code is to be used to authenticate the receiver. If the key is known to an intruder, the information might be compromised. Hence, preventive measures need to be worked upon to combat such attacks on the key of the network.

Proactive techniques are the ones that focus on the security of routing information. If the routing information such as IP address, MAC addresses and port number is known to the intruder, it may result in attacks like man-in-the-middle attack. So routing information also needs to be focused while considering the MANET security.

Reactive techniques are those techniques that focus the Intrusion Detection System (IDS) of the network which is used to monitor the flow of packets in the network. The IDS is to detect the nodes or the packets that are either sending confidential information out of the network or receiving the requests of doing so. Hence the work needs to be done on the security of nodes as well as on the information that they send and receive.

A comprehensive study has been conducted in this research article pertaining to MANET Security. The table 1 is illustrating the techniques used by the researchers to protect the Mobile Ad Hoc Network (MANET) from intruders through investigating the security parameters. The table states the role of cryptographic algorithms in the security of MANET.

Table- I: Comparative analysis of MANET Security

Technique used/ Approaches	Study Reference Number	Preventive	Proactive	Reactive		
		Key Management	Secure Routing	IDS	Packet Security	Node Security
Seniority based trust model and PGP type certification service	**[6]**	Yes	No	No	Yes	No
Most Balancing Credit Conserving (MBCC) key generation policies	[7]	Yes	No	No	No	Yes
Key management system using cluster-based group multicasting technique	[8]	Yes	No	No	No	Yes
An Anonymous Location-Based Efficient Routing Protocol	[9]	No	Yes	No	No	Yes
Hybrid security protocol using ECC, Dual-RSA and MD-5	[10]	No	Yes	Yes	Yes	No
Instant key generation mechanism	[11]	Yes	No	Yes	Yes	Yes
Secure Routing with an Integrated localised key management (SR-LKM) protocol	[12]	Yes	Yes	No	No	Yes
Energy and Mobility based Group key management scheme	[13]	Yes	No	No	No	No
Extented EAACK using One-hop ACK	[15]	Yes	No	Yes	Yes	Yes
EAACK with Elliptic Curve Cryptographic algorithm	[17]	No	No	Yes	No	Yes
Hybrid Symmetric Cryptographic Technique using AES and MD-5	[18]	No	No	No	Yes	Yes
Secure Routing protocol with security algorithms RSA, AES, DES with AODV	[19]	Yes	Yes	No	Yes	No
Secure Data transfer using AES, MD-5 and Digital signature with RSA	[20]	Yes	No	No	Yes	Yes
S-AODV protocol using hybrid cryptography technique using DES and RSA	[21]	Yes	No	Yes	Yes	No
EAACK Intrusion Detection and Prevention System using RSA and DSA	[22]	Yes	No	Yes	No	No
EAACK with AES, RSA and DSA	[23]	Yes	Yes	Yes	Yes	No
IDS using RSA, AES and MD-5	[24]	No	Yes	Yes	Yes	Yes
IDS using RSA algorithm	[25]	No	No	Yes	Yes	Yes
EAACK with AES and RSA	[26]	No	No	Yes	Yes	No

The table states that most of the research has been focused on reactive measures and least focus is drawn towards proactive category. The year-wise categorization of the techniques worked upon is presented in Table 2.

Table- II: Year-wise distribution of techniques

Year of Publication	Number of papers		
	Preventive	Proactive	Reactive
2008-09	1	0	1
2010-11	1	0	1
2012-13	0	1	2
2014-15	8	4	11
2016-17	1	2	4

The analysis can be drawn from the above table that the reactive measures which include the traffic monitoring and node behavior analysis of the network were the spotlight of the recent research. Routing information security is a research gap that needs to be worked upon in near future.

The study graph based on the above table has been drawn which reveals that the issues in key management, security of nodes and data transferred have been worked upon thoroughly. Some of the recent studies proposed new parameters that are the scope of future work to be done in MANETs. A comparative analysis in terms of security parameters have been presented in Figure 1.

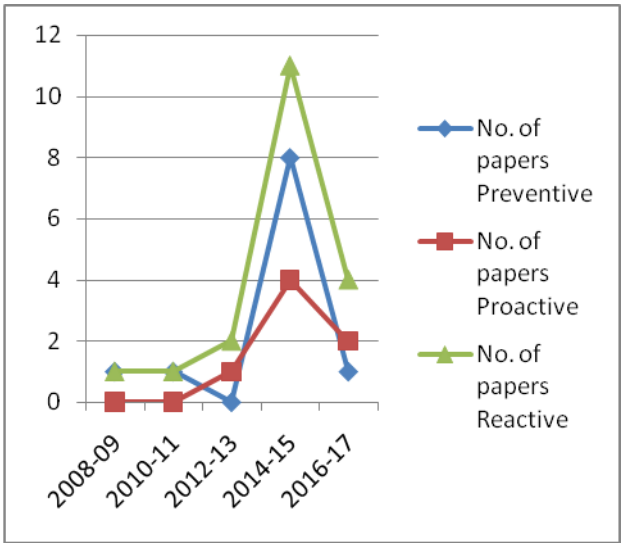

Figure- I: Comparative Analysis of recent study on MANET security.

The next section presents conclusion to the study conducted here along with future directions in the domain of MANET security.

IV. CONCLUSION

The research conducted here explicates the role of cryptographic algorithms in the security of MANET. The security parameters like node security, key management, routing protocol security, IDS and packet security have been analyzed thoroughly. *It has been inferred that the node level security have been focused, but implementing security at routing level has been over looked that poses a major threat to confidentiality of information in routing phase.* Crucial cryptographic approaches need to be used in the security of routing information so as to reduce the risk of losing the confidential data at this level of network. *Factors like energy consumption at nodes, attack prevention, packet dropping and packet delay need to be worked upon in near future.* In conclusion, the MANET security can be improved rigorously by exploiting cryptographic approaches like RSA and AES that are proven safe from attacks as per study conducted in recent past. *Besides, hashing techniques can be used to reduce the risk of security at various levels of network because hashing is the technique that compares the hashed code generated at the sender level with the code generated at the receiver level that assists in capturing details pertaining to compromising of the network information with ease*.

REFERENCES

1. R. Sheikh, M.S. Chandel and D.K. Mishra "Security Issues in MANET: A Review", IEEE, 2010. DOI: 10.1109/WOCN.2010.5587317
2. S. Kumar, G. Pruthi, A. Yadav and M. Singla "Security protocols in MANETs", Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012. DOI: 10.1109/ACCT.2012.101
3. S. B. Sharmaand and N. Chauhan "Security issues and their solutions in MANET", 1st International Conference on Futuristic trend in Computational Analysis and Knowledge Management, IEEE, 2015. DOI: 10.1109/ABLAZE.2015.7155013
4. M.Umaparvathi, Dr.D.K. Varughese "Evaluation of Symmetric Encryption algorithms for MANETs", IEEE, 2010. DOI: 10.1109/ICCIC.2010.5705754
5. Kaur and A. Singh, "An Encryption Scheme based on AES and SHA-512", IJAERV, 2015
6. M. Razi and J. Quamar "A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET", IEEE, 2008. DOI: 0.1109/ISBAST.2008.4547670
7. H. Al-Zubaidy, I. Lambadaris, Y. Viniotis, C. Huang and R.H. Hwang "Optimal Key Generation Policies for MANET Security" The direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010. DOI: 10.1109/GLOCOM.2010.5683129
8. H. Dey and R. Datta "Transmission-Efficient Group-key Generation in Large Dynamic MANET Environments", Third International Conference on Emerging Applications of InformationTechnology (EAIT), IEEE, 2012. DOI: 10.1109/EAIT.2012.6407965
9. H. Shen and L. Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE Transactions on Mobile Computing, IEEE, vol. 12, 2013, pp. 1079-1093.
10. K. Ramya, B. David , H. Shaheen, "Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET", IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-8727, 1st ed. vol. 16, 2014, pp 32-36.
11. K.S.Dhanalakshmi, Dr.B.Kannapiran and A.Divya, "Enhancing MANET Security Using Hybrid Techniques in Key Generation Mechanism", International Conference on Electronics and Communication System (ICECS), 2014. DOI: 10.1109/ECS.2014.6892809
12. S.H. Talawar, S. Maity and R.C. Hansdah "Secure Routing with an Integrated Localized Key Management Protocol in MANETs", 28th International Conference on Advanced Information Networking and Applications, IEEE, 2014. DOI: 10.1109/AINA.2014.74
13. M.R. Priyadharshini, S. Prasanna and Dr.N. Balaji "Energy and Mobility Based Group Key Management in Mobile Ad Hoc Networks", International Conference on Recent Trends in Information Technology, IEEE, 2014. DOI: 10.1109/ICRTIT.2014.6996130
14. S. Sivaranjani, S. Rajashree, "Secure Data Transfer In MANET Using Hybrid Cryptosystem", International Conference on Information Communication and Embedded Systems, IEEE, 2014. DOI: 10.1109/ICICES.2014.7033812
15. D. Sandhiya K. Sangeetha and R.S. Latha "Adaptive ACKnowledgement Technique with Key Exchange Mechanism for MANET", International Conference on Electronics and Communication Systems (ICECS), IEEE, 2014. DOI: 10.1109/ECS.2014.6892733
16. P. Joshi, P. Nande, A. Pawar ,P.Shinde,R.Umbare "EAACK - a secure intrusion detection and prevention system for MANETs", International Conference on Pervasive Computing (ICPC),IEEE 2015. DOI: 10.1109/PERVASIVE.2015.7087032
17. P.D. Nikam and V. Raut, "Improoved MANET security using Elliptic Curve Cryptography and EAACK", International Conference on Computational Intelligence and Communication Networks, IEEE, 2015. DOI: 10.1109/CICN.2015.221
18. V.Umadevi, C.Chandrasekar, "Removal of Malicious Attacks using Hybrid Symmetric Cryptographic Technique", International Journal of Computer Applications, vol.132, 2015. DOI: 10.5120/ijca2015907445
19. Prof.B.N. Jagdale and M.S. Patil, "Emulating Cryptographic Operations for Secure Routing in Ad-hoc Network", International Conference on Pervasive Computing (ICPC), IEEE, 2015. DOI: 10.1109/PERVASIVE.2015.7086969
20. R.K. Kapur and S.K. Khatri "Secure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography", IEEE, 2015. DOI: 10.1109/ICRITO.2015.7359293
21. Sharma, D. Bhuriya and U. Singh "Secure Data Transmission on MANET by Hybrid Cryptography Technique", International Conference on Computer, Communication and Control, IEEE, 2015. DOI: 10.1109/IC4.2015.7375688
22. S. Awatade and S. Joshi "Improved EAACK: Develop Secure Intrusion Detection System for MANETs Using Hybrid Cryptography", International Conference on Computing Communication Control and Automation, IEEE, 2016
23. A.A. Patil and S. Mali, "Hybrid Cryptography Mechanism for Securing Self-Organized Wireless Networks", 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2016.

24. V.B. Joshi and R.H. Goudar, "Intrusion Detection Systems in MANETs using Hybrid Techniques" International Conference on Smart Technology for Smart Nation, IEEE, 2017.
25. Sankaranarayanan.S and Murugaboopathi.G "Secure Intrusion Detection System In Mobile Ad Hoc Networks Using RSA Algorithm" Second International Conference on Recent Trends and Challenges in Computational Models, 2017.
26. S.Vimala and Dr.S.K.Srivatsa "Security using data compression in MANETS", 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB17) IEEE, 2017

AUTHORS PROFILE

Ms. Veerpal Kaur completed her B.Tech and M.Tech from Lovely Professional University in year 2014. She started her career as Assistant Professor, CSE Department, Saraf Institute of Engineering and Technology. She has her M.tech dissertation in domain of Network and Security and has extended her guidance to students for their project work in the domain of security. She has few publications that have been indexed in scopus database. Currently, she is working as Assistant Professor, DCSE, Chitkara University. She is faculty advisor of IEEE CIET student branch inspiring students to develop projects for the society. She has been keenly working on security of networks. For more information, contact @ veerpal.kaur@chitkara.edu.in

Dr. Kamali Gupta did her B.tech from Y.M.C.A Institute, Faridabad in 2007 and received her M.Tech and Ph.D degree from Maharishi Markandeshwar University, Mullana. She initiated her career with Infosys Technologies Limited as System Engineer. Subsequently, she extended her services to Geeta Institute of Management and Technology, Kurukshetra and Maharishi Markandeshwar University, Sadopur, Ambalaand. Currently, she is working as Associate Professor, DCSE, Chitkara University. She has guided many M.Tech thesis and is currently guiding many Ph.D Scholars She underwent numerous MOOC course certifications and her profile carries various Microsoft certifications. She has many professional affiliations to her credit. She is having a rich experience in domain of university accreditations and other institutional workloads. She has been fortunate enough to host two Tedx conferences and has wide exposure in institutional event management. She has written a number of research publications that have been indexed in acknowledged databases. Her research interests include cloud computing, security and data structures. For more info, reach @ kamaligupta13@gmail.com, kamali.singla@chitkara.edu.in.

Dr. Vidhu Baggan graduated at Beant College of Engineering & Technology and completed her Master's Degree at NITTTR, Chandigarh.She did her Ph.D from Chitkara University, Punjab,India. She has a teaching experience of more than18 years. At present, She is Associate Professor at Department of Computer Science & Engineering, Chitkara University, Punjab. In addition, She is certified as a Microsoft Certified Professional (2004), Cisco Certified Network Associate(2005 & 2016), Huawei Certified Network Associate(2018) and Huawei Certified Instructor(2018). She has many research publications to her credit. Her core interest areas are domains of networking. For more information, reach her at vidhu.baggan@chitkara.edu.in.

Gagandeep Kaur did her B.tech from Swami Vivekanand Institute of Engineering and Technology, Banur in 2014 and received her M.Tech from Punjabi University, Patiala. She initiated her career with Chitkara University as Assistant Professor. Currently, she is working as Assistant Professor, DCSE, Chitkara University. She has many professional affiliations to her credit. She is having a rich experience in domain of institutional workloads and performed many departmental duties. She has written a number of research publications. Her research interests include Data Mining, Machine Learning, Computer Architecture and Artificial Intelligence. For more info, reach @ gaganmalhotra1791@gmail.com.

Ms.Aman jyoti did her B.tech from B.C.E.T. Institute, Gurdaspur in 2012 and received her M.Tech from Punjabi University, Patiala in 2015. She initiated her career with BCS Solutions as Trainer. Currently, she is working as Assistant Professor, Department of Computer Science & Engineering, Chitkara University. She has many professional affiliations to her credit. She is having a experience in domain of departmental duties and other institutional workloads. She has written few research publications. Her research interests include network security and machine learning. For more info, reach @ amanjyot20@gmail.com.