ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

Hybrid Cryptography Approach for Securing MANETs – A Survey

Zuhi Subedar [1], Satish Deshpande [2]

P.G. Student, Department of Electronics and Communication Engineering, Gogte Institute of Technology, Khanapur Road, Karnataka, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Gogte Institute of Technology, Khanapur Road, Karnataka, India[2]

ABSTRACT: In networking, the use of Mobile Ad-hoc Networks (MANETs) has been increasing tremendously since last decade. The reasons being that it doesn't require any infrastructure and the nodes in the network configure itself on the fly without strict network administration. However, these ad hoc networks are susceptible to various attacks at almost all layers, mainly the network layer. To provide defence against these attacks we need to use certain cryptographic techniques and Intrusion Detection Systems (IDS). In this paper, we present survey of various routing protocols and cryptographic algorithms used in MANETs that could deal with a single type of attack or a range of attacks.

KEYWORDS: MANETs; attacks; security; routing protocols; cryptographic algorithms

I. Introduction

Mobile Ad- hoc Networks (MANETs), also known as Wireless Ad-hoc Network [1] or Ad-hoc Wireless Network, is an infrastructure-less network where the mobile devices are associated wirelessly as shown in Fig.1[2][3].

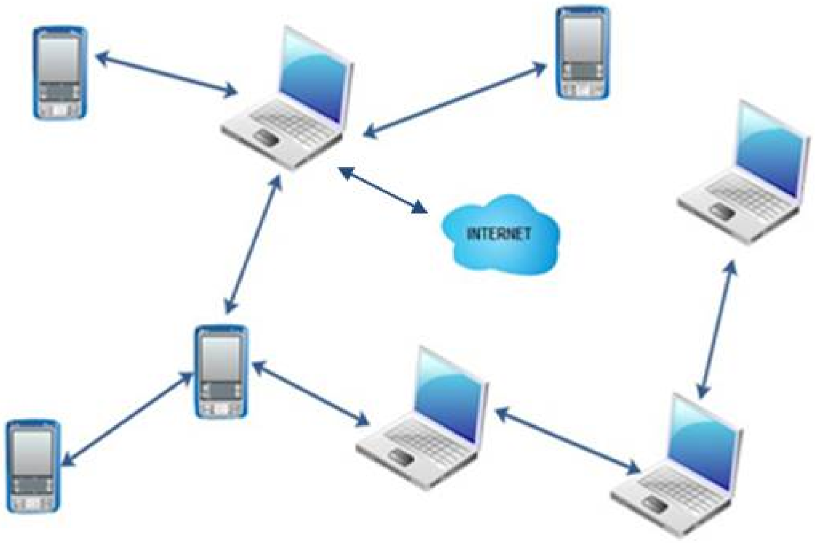

Fig.1. Adhoc Network architecture

These networks self configure themselves continuously because the devices in a MANET can move freely in all directions and hence its links with other devices keep changing repeatedly. Hence, each device can be considered to be a router which forwards traffic that is not related to its use.

These networks find applications in various fields such as military, weapons, air, navy, health, disaster management, environment sensors etc., [4].

As the nodes in MANET change their positions continuously, their topology also changes and hence different algorithms must be used for different network structure. Apart from applications of MANETs in various areas, they also suffer from several security threats like dropping of packets, selfishness, QoS provisioning etc., and so several security mechanisms need to be incorporated to combat these threats and so cryptographic mechanisms are used to prevent the network from being attacked by external entities. However, to prevent attacks caused by internal entities, an altogether different mechanism has to be used [4].

II. Background

An Internet is an interconnection of several networks and maintaining security of these networks is a major concern and need of every organization. One of the major challenges faced by these networks is; the networks that are responsible for transporting voice and data are vulnerable to various attacks, monitoring and interception [5].

Hence, there has to be a way to protect the network to prevent the useful information from getting to unauthorized access, and therefore several security mechanisms like authentication, encryption algorithms, digital signatures and security services like authentication, data confidentiality, access control, data integrity and so on are used to detect, protect, prevent or recover transported data over a network from an attack [6].

A. *Authentication*:

It is the process of guaranteeing authenticity of communication i.e. verifying the identity of the user. Two authentication services as defined in X.800 are Peer entity authentication and Data origin authentication where the former deals with checking validations of communicating entities and the later deals with validating the source of data.

Some types of functions used to produce an authenticator are:

- Message encryption: In this, the cipher text serves as an authenticator.
- Hash Function: The function that maps any length message into a fixed length hash value serves as an authenticator.
- Message Authentication Code: The function of the secret key along with message that produces a fixed length value serves as an authenticator [6].

B. *Cryptography:*

Cryptography is a process of converting plaintext to cipher text and vice versa. Fig.2 shows different types of cryptographic techniques.

1. *Symmetric Cryptography:*

In symmetric Cryptography, a single key is used for encrypting and decrypting a message which is shared between the two parties involved in communication. From the figure we can note that Symmetric cryptography consists of DES in which the data is encrypted using 64 bit blocks using 56 bit key. This algorithm transforms 64 bit input into 64 bit output in series of steps and AES which was published to replace DES. AES is a block cipher which uses 128 bit block size with a key size of 128,192 or 256 bits. AES consists of several rounds wherein each round consists of four functions namely, byte substitution, permutation, arithmetic operations over finite field and then finally XOR operation with a key [6].

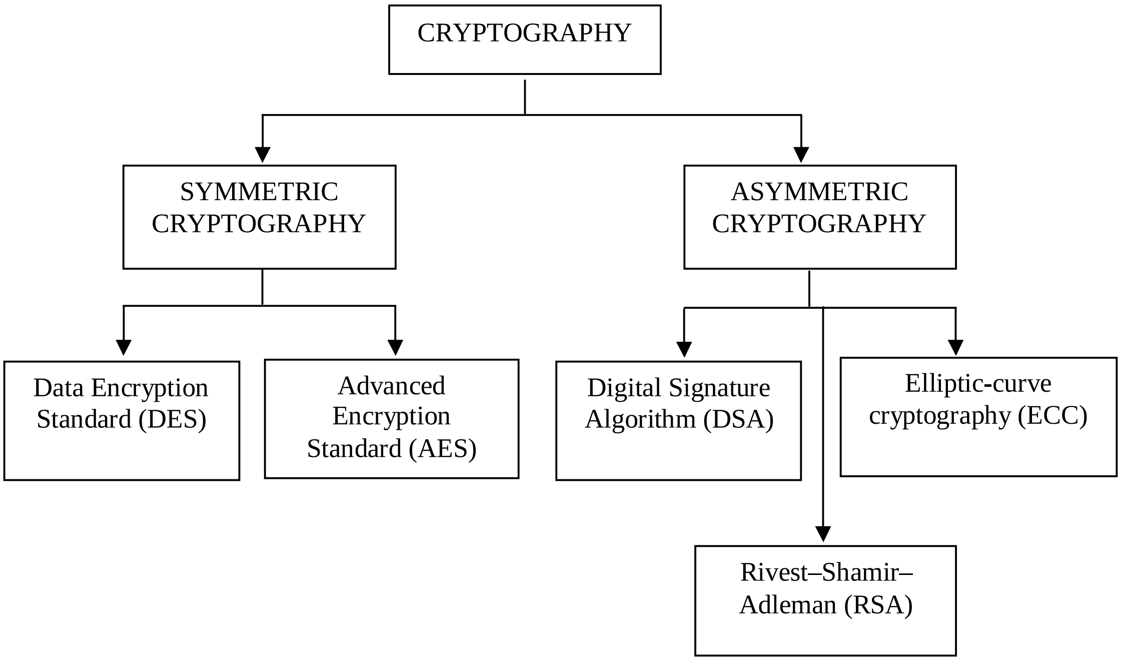
CRYPTOGRAPHY
SYMMETRIC CRYPTOGRAPHY
ASYMMETRIC CRYPTOGRAPHY
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
Digital Signature Algorithm (DSA)
Elliptic-curve cryptography (ECC)
Rivest–Shamir–Adleman (RSA)

Fig.2. Types of Cryptography

1. *Asymmetric Cryptography:*

In asymmetric/public key Cryptography, two different keys are used. One is called a private key which is known by a single party and a public key available to both the parties involved in communication. The public keys are shared among the parties by means of key management mechanism that is Diffie Hellman Key distribution.

Asymmetric cryptography includes DSA, RSA and ECC [6]. ECC is preferred more compared to RSA and/or DSA because of its smaller key size and faster computation speed. The following Table.1 depicts the comparative study of ECC, RSA/DSA and symmetric crypto based on their key sizes.

Table.1. Comparable key sizes of Symmetric, ECC and RSA/DSA [6]

Symmetric **(Key size in bits)**	**ECC** **(size of n in bits)**	**RSA/DSA** **(modulus size in bits)**
56	*112*	*512*
80	*160*	*1024*
112	*224*	*2048*
128	*256*	*3072*
192	*384*	*7680*

C. ***Routing in MANETs:***

Routing is the decision making to direct network packets from the source to destination. Routing can be either static or dynamic. In static routing, routing tables are configured manually and routing of packets is done using these tables, usually smaller networks use static routing, Public switch telephone network is one example that uses this kind of routing. Dynamic Routing makes use of routing tables that are constructed automatically using routing protocols. Some dynamic routing protocols are Open source Shortest Path First (OSPF), Routing Information Protocol (RIP) and so on [15].

1. ***The major challenges faced by routing protocols in MANETs are:***

- Location dependent contention: The channel assertion increases with increase in the number of nodes. Higher the argument value greater is the rate of concussion which results in the annihilation of the bandwidth.
- Bandwidth constraint: All the nodes in the network share a single channel hence bandwidth depends on the number of nodes for that link and the measure of traffic that link can contend. Hence only a small amount of bandwidth gets used by every node in the network.
- Mobility: Since MANETs are mobile networks they have nodes which are mobile whose major problems are packet collisions, state routing information, transitory loops, habitual path breaks, and knots with reservation of expedients for the node and the link.
- Error prone and shared channel: The bit error rate for wired network is very low assimilated to wireless networks. Hence routing protocols should take into deliberation of Signal to noise ratio, path loss, and state of the link thus upgrading the overall efficacy of the network.
- Other constraints: This entails the battery power, reckoning power, buffer storage, etc., [15].

2. ***The major requirements of a routing Protocol are:***

- Loop-free routing: A routing protocol should be well schemed to deter transient loops, take remedial actions, evade unnecessary desolation of bandwidth, etc.,
- Scalability: Deals with how efficiently the network is prosecuting. For a network to be scalable it should acclimate to the network size, and has inferior control overhead.
- Security and privacy: The network should be resilient to vulnerabilities and perils with capability to elude DoS attack, impersonation assaults and resource consumption.
- Quick route reconfiguration: Since there are unpredictable changes in the network the protocol should be very efficacious in finding a fresh route or reconfiguring the route.
- Minimum route acquisition delay: The route procurement delay for a node that does not have a course to the destination ought to be very low [15].

D. ***Routing Protocols in MANETs:***

Routing protocols in MANET are classified proactive or table driven, reactive or on-demand and hybrid as shown in Fig. 3. Proactive maintains a list of updated destinations and their routes by periodically distributing the routing tables throughout the network but the main limitation of this kind of protocol is the periodic maintenance of routing table updation when network change occurs. Reactive is also termed as source initiated protocol in which routing information updation is not required hence it imposes minimum overhead but faces high latency problem. Hybrid is the combination of the advantages of table driven and on-demand protocols.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

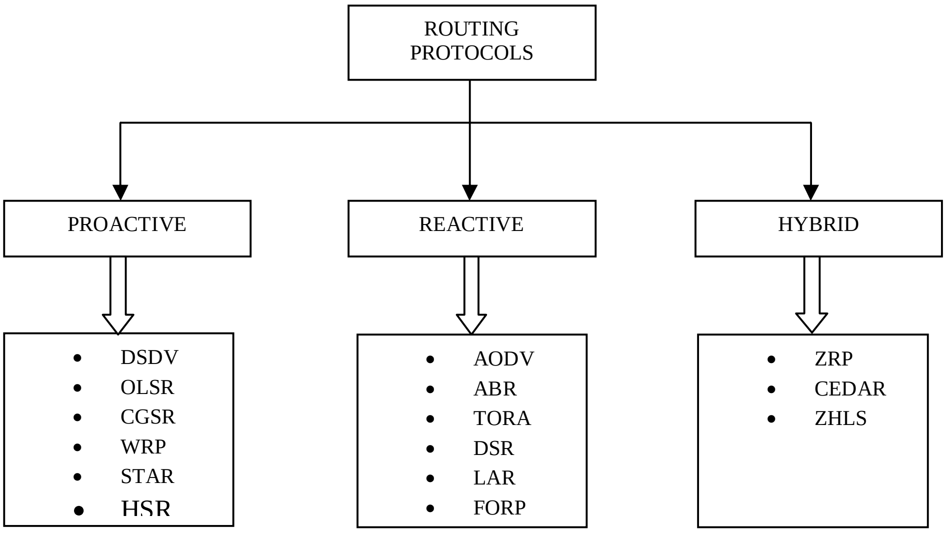

Fig.3. Types of Routing Protocols [7].

Table.2 provides a brief comparative analysis of various routing protocols as shown below.

Table.2. Comparative study of Routing Protocols [15].

Protocols	Protocol Type	Advantages	Disadvantages
DSDV	Table Driven	Less delay, Adaptable	High Control Overhead
CGSR		Better bandwidth utilization	Multiple path breaks due to frequent change of cluster head
WRP		Faster Convergence, less delay, adaptable	Requires large memory, greater power supply
OLSR		Less control overhead, low connection setup time	-
STAR		Low Communication Overhead	-
DSR	On demand	Minimum Control Overhead	High Connection set up delay
AODV		Less connection set up delay	Heavy control overhead, unnecessary bandwidth consumption
TORA		Less control Overhead	Formation of non-optimal routes
LAR		High BW utilization, less control overhead	-
ABR		Stable routes, fewer path breaks	High delay during route repair
ZRP	Hybrid	Minimum control overhead	Overhead increases with increase in overlapping of nodes in routing zones
CEDAR		Efficient routing and QOS path computation	Updation increase control overhead
ZHLS		Reduced storage requirements, robust and resilient to path breaks, non overlapping zones	Path to destination is suboptimal

III. Related work

In the paper titled, “Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's” authored by Prachi D. Gawande and Yogesh Suryavanshi, On-Demand Routing Protocol based cryptographic system for MANET is put forth. The routing protocols accustomed here are AODV and DSDV. The AODV protocol has characteristics which conquer the disbenefits of DSDV like steady updation of routing tables which exploits up battery power and a small amount of bandwidth even when the network is inert and whenever the topology of the network varies, a fresh sequence number is mandatory before the network re-converges; thus, DSDV is not befit able for highly dynamic or large scale networks. AODV is the one which is most adaptable and better functioning routing protocol compared to DSDV. The technique used here for securing network is RC6 (Rivest Cipher 6) [8].

In the paper titled “An Intrusion Detection System for Wireless Sensor Networks” authored by Ilker Onat and Ali Miri, A detection based security plot for wireless sensor network is advanced. Since sensor nodes have low communication capability and due to specific properties like maintenance of neighbourhood information which makes anomaly spotting easier. Such characters empower to provide security to large scale networks easily. Here a simple dynamic statistical model is built and also a low complex mechanism is used to control the power levels and the arrival rates of the received packets [9].

In the paper titled, “A Study of Intrusion Detection Systems in MANETs” authored by Umesh Prasad Rout, presented a detailed study on different Intrusion Detection systems. Stand alone Intrusion detection runs on each node self dependent to find any malignant node present. He also presented novel IDS which uses OLSR protocol for MANET which offers several serious liabilities which could lead to paralyse the communications within the network like passive eavesdropping, usurpation, routing disruption or denials of service (DoS) [10].

In the paper titled, “A Novel Intrusion Detection System for MANETS” authored by Christoforos Panos, Christos Xenakis and Ioannis Stavrakakis, A novel intrusion detection framework is proffered for MANETs which is a combination of walk based IDS tactic and multi layer specification based identification engine. The proposed architecture assesses less processing and communication overhead to the underlying network, it assorts uniformly the proceeding workload among the network nodes, and it is well-conditioned to dynamic network changes. Moreover, it does not create points of defaults, and it is not vulnerable to man-in-the-middle and blackmail attacks. On the other hand, the proposed engine enables the detection of both known and unknown attacks, and mitigates the need for a signature database. Finally, it is not prone to high rates of false alarms [11].

In the paper titled, “EAACK—A Secure Intrusion-Detection System for MANET’s”, authored by Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, a new intrusion-detection system titled Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK substantiates higher malicious- behaviour-detection rates in certain circumstances while does not greatly affect the network interpretations. DSA and RSA algorithms are accustomed for finding out malicious attacks. From the result section it is clear that with respect to network overhead and signature size DSA is better compared to RSA. But DSA consumes more computation power as compared to RSA [12].

In the paper titled, “A Novel Approach towards the Detection of Malicious Nodes in Mobile Ad Hoc Networks” authored by Anup Ashok Patel and Shital Mali, a novel intrusion detection system called Secure Enhanced Adaptive Acknowledgement (SEAACK) is proposed. The proposed system deals with the issues related to the existing IDS and deter the malicious nodes more effectively than the existing system under certain circumstances while not greatly affecting the network performances. From simulation results proposed system exhibits higher packet delivery ratio of about 94%which is far better as compared to other existing systems, throughput which is nothing but the amount of data received at the destination of proposed system is much greater of about 780.8 Kbps than the existing systems and routing overhead which is ratio of amount of routing related transmissions, supposed to be as small as possible for better network performance but there is slightly increase in the routing overhead of proposed system which is 2.62 due to the adaptation of digital signature [4].

From the papers [13] [14], there are few specific routing algorithms like AODV, DSDV, ZRP, DSR etc., AODV DSDR and DSR protocols are preferred more in the implementation of Mobile Adhoc Networks.

IV. Conclusion

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network. As the performance of the proposed algorithm is analyzed between two metrics in future with some

DOI: 10.15680/IJIRCCE.2018. 0601024

modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

V. Future Work

Our future work mainly concentrates on the enhancement of MANET and its core issues such as end-to-end delay, throughput etc., by analysing the performances of most preferred routing protocols with cryptographic techniques.

References

1. "Wireless ATM & Ad Hoc Networks", Kluwer Academic Press, *1997.*
2. Zanjireh, M M., and Hadi Larijani., "A survey on centralised and distributed clustering routing algorithms for WSNs.", In Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st, pp. 1-6. IEEE, 2015.
3. Toh, Chai K., "Ad hoc mobile wireless networks: protocols and systems", Pearson Education, 2001.
4. Patil, A A. and Mali, S., "A Novel Approach towards the Detection of Malicious Nodes in Mobile Ad Hoc Networks", International Conference on Communication (ICCT), pp. 12-16, September 2015.
5. https://www.scmagazine.com/top-10-security-challenges-for-2017/article/682314/
6. William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.
7. Lalar, S., and Yadav,A., "Comparative Study of Routing Protocols in MANET", OJCST 10 (2017): 174.
8. Gawande, P. D., and Suryavanshi, Y., "Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's", IEEE ICCSP, pp 1478-1481, 2015.
9. Onat, I., and Miri, A., "An Intrusion Detection System for Wireless Sensor Networks", International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE, August 2005.
10. Rout, U.P., "A Study of Intrusion Detection Systems in MANETs", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 2 pp 86-92, February 2013.
11. Panos, C., Xenakis, C., and Stavrakakis, I., "A Novel Intrusion Detection System For MANETS", Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE Athens, Greece, 2010.
12. Shakshuki, E. M., Kang, N., and Sheltami, T. R., "EAACK— A Secure Intrusion-Detection System for MANETs", IEEE Transactions on industrial electronics, vol. 60, no. 3, pp 1089-1098, March 2013.
13. Manickam, P., Baskar, T. G., Girija, M., and Manimegalai, D. D.,"Performance Comparisons of Routing Protocols in mobile adhoc networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011.
14. El Khediri, S., Nasri, N., Benfradj, A., Kachouri, A., & Wei, A., "Routing protocols in MANET: Performance comparison of AODV, DSR and DSDV protocols using NS2", IEEE, 2014.
15. Murthy, C.S.R., "Ad-hoc Wireless Networks: Architectures and Protocols", 2004.

Biography

Zuhi Subedar is a PG student perceiving Masters in Digital Communication Networking., KLS Gogte Institute of Technology, Belagavi, Karnataka, India. She received Bachelor of Engineering degree in Electronics and Communication from Jain College of Engineering, Belagavi, Karnataka, India in the year 2014. Then she worked in the corporate sector for 1.7 years. Her research interests include network security, cryptography and web services.

Satish P. Deshpande is working as Assistant Professor in the Dept. of E&C Engg., KLS Gogte Institute of Technology, Belagavi, Karnataka, India. He completed Bachelor of Engineering in Electronics in the year 1991. Then he worked in service industry for 08 years. He joined education field in the year 1999. He completed M.Tech in Digital Communication Networking. Currently, he is pursuing his Ph.D. in the field of Measurement Techniques and Instrumentation. He has published many papers in Journals and Conferences.