ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 5, May 2016

Security Enhancement of QOS-based robust multipath routing Protocol (QRMR) using Elliptic Curve Cryptography Algorithm: A Review

Monika Rani, Dr. Sunil Kumar Nandal

Abstract- **This review paper is about study of different routing protocols which is used in MANET/ad-hoc n/w. to select that type of protocol which adopt topology change easily. Because today requirements of users increase rapidly they wants connecting during moment. Main challenges the MANET is proving good QOS, security and resource reuse.**

Main context:- introduction, routing protocols, QOS routing protocols, type of attacks.

I. Introduction

Network means connection of two or more computer & device. It may be wired or wireless. N/w is used for transfer information from one computer to another computer. Wired connection is used transmission media like coaxial cables, fibers cable etc.[1], [2]but in wireless connection device are connected with each other without any transmission media these are communicated with the help of radio waves. For example Bluetooth, Wi-Fi, mobile calls etc. Nowadays users requirements are increasing they wants to use their devices like laptop, pads etc. anywhere & anytime when they required. [3]

As beliefs networks usually used to be fixed at certain geographic locations, wireless technology is becoming more popular & important. User wants to stay connected when they are in moving state. Wireless n/w provided that freedom to users which they want.

Monika Rani, M.tech(Computer Science),Guru Jambheshwar University of Science & Technology, Hisar Hisar, Haryana

Dr. Sunil Kumar Nandal,(Assistant Professor)CSE dept. Computer Science,Guru Jambheshwar University of Science & Technology, Hisar, Haryana

There are many way to classify wireless networks, depending on: Architecture type and the size of the network. [1]

Wireless n/w are roughly divided into two parts

- Framework dependent networks
- Ad hoc wireless networks

II. Ad-hoc network

The ad hoc wireless network is a special case of wireless network has not any fixed framework. This is a type of MHWN. In this according to demand & requirement, it creates virtual network. It is a decentralized n/w. This feature of the wireless ad hoc networks makes it flexible and quickly deployable. Nevertheless, significant technological challenges are also posed by this property. MANET is a type of ad-hoc network.

Mobile ad-hoc network(MANET):-

MANET is a type of ad hoc n/w. MANET is a group of wireless mobile nodes which [2] can be connected when any user required.[It is decentralize infrastructure & not preexisting [3]. Every node in the n/w is may be source & destination & routers itself for transfer information. A MANET is an autonomous system of mobile routers connected by wireless links the union of which form an arbitrary graph. Ad-hoc n/w is having dynamic technique nodes may be move in the n/w and change their physical location.[8]

III. Challenges in MANET

There are many problems in MANET n/w due to not fixed framework & infrastructure. It is very difficult to maintain routes for destination. Routing, Quality of services Resources, maintenance route, Security, Sleep period operation, Multicasting, Loop free, Multiple routes[7]

Routing:-

Basically routing is a technique through which we find the routes[8] for transmission information from source to destination. In the past, the term **routing** also used to transfer network traffic among networks. Mainly there are 3 type of routing protocol.[4]–[6]

1. Pro-active (table-driven) routing:- every node make a routing table which have destination and route from the source[13].

Disadvantage: - extra space required for maintained tables. Slow speed of restructuring

Examples:- AODV(ad-hoc on demand distance vector), DSR(dynamic source routing) etc.

2. On demand(reactive) routing :- find a route by sending a RREQ [3], [7]msg this protocol needs less touting information

Disadvantage: - no of request packet is increasing if no of nodes are increasing,

Examples:- DSDV(distance sequential distance vector), OLSR(optimized link state routing) etc.

3. Hybrid protocols:- it is basically take advantages of both protocols. Advantage of these protocols depends upon the no of nodes which are active that time.

Examples: - ZRP(zone routing protocol),ZHLR**(**Zone-Based Hierarchical Link State Routing) etc. Routing help the user finding shortest path from source to destination.[8], [9]It is very important component in MANET communication because there are no fixed infrastructure and no fixed size of nodes. MANET is having dynamic topology nodes may be change their position cautiously so we required that protocols which adopt topology changes easily.

Quality of services:-

Quality of services means that collection of data from different users which measure degree of the user satisfaction from services.[10], [11]QOS is very important component in the n/w. it means that how better our data is transfer from source to destination. It is a very difficult[1], [2], [12] task to select/find shortest path from source to destination with the help of routing protocols keep in mind that quality of the series may not be decrease.

Challenges while using QOS in adhoc network:-

- Undependable channel
- Movement of nodes
- Limitation of energy supply
- No centralized approach
- Channel disarrangement
- Security

Type of QOS routing protocols:-

- Network topology based protocols[13]–[15]
    1. Flat protocols:- mostly routing protocols implemented on physically flat n/w infrastructure with mobile users of same group. AQOR (ad hoc QOS on demand routing), QAODV (QOS AODV) etc.
    2. Hierarchical protocols:- for infrastructure based multicast routing protocols using physically hierarchical infrastructure for different type of mobile nodes. HQRMP(Hierarchical multicast routing protocol), SOM (self-organizing map)
    3. Location aware (hybrid):- connected through Bluetooth when required. LGF(location-based geo casting & forward) , SPBM(scalable position based multicast)
- Route discovery with QOS approach
- Based on connection of mac layer & n/w
    1. Dependent protocols:- in this n/w layer is dependent upon the mac layer. NSR (node state routing), CCBR (capacity- based routing) etc.
    2. Independent protocols:- in this n/w layer is not dependent upon the mac layer. QOLSR (QOS optimized link state

routing), DSARP (delay-sensitive adaptive routing protocol) etc.

- QOS matric base:-

  1. Single constrained: - only using single parameter for improving QOS CACP (Content admission control routing protocols), CAAODV (Contention-Aware AODV) etc.
  2. Multi constrained: - to find the multiple feasible path for communication GAMAN (genetic algorithm based routing), AAQR (application aware QOS routing protocol) etc.

- QOS guarantee:-

  1. Soft QOS approach:- guarantee of QOS in certain services only CLMCQR (Cross Layer Multi-Constraint QOS routing), AAQR (application aware routing protocols) etc.
  2. Hard QOS approach:- guarantee of QOS is compulsory NSR(Node State Routing), MRPC (Maximum Residual Packet Capacity routing) etc.

Main propose of QOS is determined a route from source node to destination that fulfill the needs of users with QOS. Route is selected on the bases of QOS desire.

Security:-

Security is very important part of any transmission due to [6]open source nature of wireless n/w. time data is very private like in banking & army information. So we applied security our data is very important task[9]. Type of attacks in wireless n/w.

- Denial of services:- due to accidental failure of nodes, dos attacks try to misuse of resource of failure nodes by sending extra & unrequired msg[9]
- Attacks on information in transmission:- nature of n/w is open source any hacker can sense the flow and can interrupt or edit the packets
- Sybil attacks:- due to this attack effect distributed storage routing algorithm, data aggregation, in detection tech
- Wormhole attack:- at one location attacker record the packet and transmitted data after editing to the destinations.[6]

Cryptography:- it is a type of secure the data by encryption decryption it is not mainly for wireless n/w. first generation of cryptography algorithm is RSA. But ECC algorithm is used in wireless sensor n/w for achieved n/w security.

ECC algorithm is used in case of key exchanges by[1] certificate authority (CA) to share the public key certificates with end users. Elliptic Curve Cryptography is[4] a secure and more efficient encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA.

There are three steps in the process

- key generation,
- encryption
- decryption

Advantages of ECC over RSA :

1. Shorter keys are as strong as long key for RSA.

2. Low on CPU consumption.

3. Low on memory usage.

4. Size of encrypted data is smaller

IV. Proposed model

ECC algorithm is used firstly only for single route discover algorithm, if that path is busy then delay in transmission [16]is increase because it is waiting until the route is free. It is further implemented for the multiple path discover algorithm for overcome the delay and waiting route for transmission and compression with the exiting technique.

V. Conclusion

In this paper we review about ad-hoc n/w, MANET, challenges in MANET, routing protocols and QOS routing protocols, security, different type of attacks, ECC algorithm and advantages of ECC algorithm over RSA algorithm. This paper help to further studying about the ad-hoc n/w and challenges in MANET. The future scope of this paper is to more detailed study about QOS routing protocols which are described in the paper. Many research issues and topics like control techniques & protocols, QOS protection under non-success transmission, QOS support for multicast task, security by denial services attacks further research topics.

VI. *References*

[1] S. Chakrabarti and A. Mishra, "QoS issues in ad hoc wireless networks," *IEEE Commun. Mag.*, vol. 39, no. 2, pp. 142–148, Feb. 2001.

[2] C. R. Lin and J.-S. Liu, "QoS routing in ad hoc wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1426–1438, Aug. 1999.

[3] I. Hanzo L. and R. Tafazolli, "A survey of QoS routing solutions for mobile ad hoc networks," *IEEE Commun. Surv. Tutor.*, vol. 9, no. 2, pp. 50–70, Second 2007.

[4] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: a core-extraction distributed ad hoc routing algorithm," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1454–1465, Aug. 1999.

[5] V. N. Talooki and K. Ziarati, "Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks," in *2006 Asia-Pacific Conference on Communications*, 2006, pp. 1–5.

[6] "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET - Springer." [Online]. Available: http://link.springer.com/chapter/10.1007%2F978-1-4614-6747-2_8. [Accessed: 16-May-2016].

[7] V. Suryanarayana and M. Ambica, "A STUDY ON ADHOC NETWORK ROUTING PROTOCOLS," *IJCER*, vol. 1, no. 4, pp. 208–213, Dec. 2012.

[8] M. Ali, B. G. Stewart, A. Shahrabi, and A. Vallavaraj, "Enhanced QoS support in Mobile Ad hoc Networks using multipath routing backbones," in *2011 IEEE GCC Conference and Exhibition (GCC)*, 2011, pp. 315–318.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *10th IEEE International Conference on Network Protocols, 2002. Proceedings*, 2002, pp. 78–87.

[10] S. Chakrabarti and A. Mishra, "QoS issues in ad hoc wireless networks," *IEEE Commun. Mag.*, vol. 39, no. 2, pp. 142–148, Feb. 2001.

[11] J. L. Sobrinho and A. S. Krishnakumar, "Quality-of-service in ad hoc carrier sense multiple access wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1353–1368, Aug. 1999.

[12] S. Venkatasubramanian and N. P. Gopalan, "A QoS-based robust multipath routing protocol for mobile ad hoc networks," in *First Asian Himalayas International Conference on Internet, 2009. AH-ICI 2009*, 2009, pp. 1–7.

[13] C. Zhu and M. S. Corson, "QoS routing for mobile ad hoc networks," in *IEEE INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*, 2002, vol. 2, pp. 958–967 vol.2.

[14] "A Glance at Quality of Services in Mobile Ad-Hoc Networks." [Online]. Available: http://alumni.cs.ucr.edu/~csyiazti/courses/cs260/html/manetqos.html. [Accessed: 16-May-2016].

[15] "CORE: Connecting Repositories." [Online]. Available: https://core.ac.uk/download/pdf/26989725.pdf. [Accessed: 16-May-2016].

[16] "IEEE Xplore Abstract - Reconfigurable architecture for elliptic curve cryptography." [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5738774&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5738774. [Accessed: 16-May-2016].

Monika Rani, M.techComputer science**,**Guru Jambheshwar University of Science & Technology, Hisar, Hisar, Haryana

Dr. Sunil Kumar Nandal, (Assistant Professor)CSE dept. Computer Science,Guru Jambheshwar University of Science & Technology, Hisar, Haryana