ISSN 2320-9984

Volume 6 Issue 1| March 2018 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Result on Improved Diffie-Hellman key exchange using Elliptic Curve (IDHECC) Scheme for securing Mobile Adhoc Network Routing Data using AODV Protocol

Khushboo Kushwaha
M.Tech. Research Scholar
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: khushboo.kushwaha118@gmail.com

Deepak Agrawal
Head of the Department
Department of Computer Science and Engineering
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email:deepakagrawal@takshshila.org

Abstract—*Mobile Adhoc Network (MANET) is a large scale network with thousands of tiny sensors moreover is of utmost importance as it is used in real time applications. Currently MANET is required for up-to-the-minute applications which include Internet of Things, Smart Card, Smart Grid, Smart Phone and Smart City. However, the greatest issue in adhoc network is secure communication for which key management is the primary objective. Existing key management techniques have many limitations such as prior deployment knowledge, transmission range, insecure communication and node captured by the adversary. The proposed novel ECC and diffie-hellman key exchange algorithm provides better transmission range and secure communication. The overall network is separated into circular tracks and triangular sectors. Energy conservation Routing Protocol (AODV)was used for routing of data in MANET, which reduces the delay with increased packet delivery ratio. Further for secure routing Improved Diffie-Hellman key exchange using Elliptic Curve (IDHECC), which reduces the memory space and computational overhead than the existing Elliptic Curve Cryptography (ECC) key management scheme for Securing MANET.*

Keywords:—*Mobile Adhoc network, Routing Protocol, Key Management Scheme, Elliptic Curve Cryptography, IDHECC, AODV.*

1. INTRODUCTION

We consider the problem of congestion control in mobile ad-hoc networks (MANETs). For the different structure TCP do not work properly with the specific effects occurring in MANETs. This is because TCP has originally been designed for the Internet, a network with different properties. As a consequence, appropriate congestion control is widely considered to be a key problem for MANETs.

A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet.

Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we can imagine a group of peoples with laptops, in a business meeting at a place where no network services is present. They can easily network their machines by forming an ad-hoc network. This is one of the many examples where these networks may possibly be used.

Characteristics of MANETs

Mobile ad-hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), Omni directional (broadcast), probably steer able, or some combination thereof [1]. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hoop graph or "ad-hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

The characteristics of these networks are summarized as follows:

1. Communication via wireless means
2. Nodes can perform the roles of both hosts and routers
3. Bandwidth-constrained, variable capacity links
4. Energy-constrained Operation
5. Limited Physical Security
6. Dynamic network topology
7. Frequent routing updates

Features of Mobile Ad-hoc Networks

MANETs is an IEEE 802.11 framework. It is an interconnected collection of wireless nodes where there is no networking infrastructure in the form of base stations, devices do not need to be within each other ‘s communication range to communicate, the end -users devices also act as routers, nodes can enter and leave over time, data packets are forwarded by intermediate nodes to their final destination.

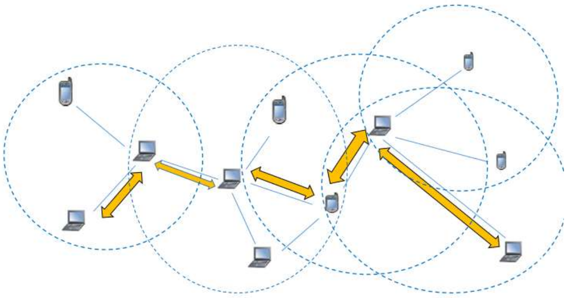


Figure 1: Mobile Ad-hoc Networks

Above Figure 1 illustrates the way of communication in between multiple hosts where if one particular node does not belong to the range of any of the other node then also it can communicate to each other by the help of any of mediator node.

2. RELATED WORK

An Overview of Routing Protocols in Mobile Ad-Hoc Network International Journal of Advanced Research in Computer Science and Software Engineering 2013 Dr. S. S. Dhenakaran.

Mobile ad hoc networks have become very popular and lots of research is being done on different aspects of MANET. Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper concentrates on routing techniques which is the most challenging issue due to the dynamic topology of ad hoc networks. There are different strategies proposed for efficient routing which claimed to provide improved performance. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions. This paper provides an overview of different routing protocols proposed in literature and also provides a comparison between them.

In this paper a number of routing protocols for MANET, which are broadly categorized as proactive (TableDriven) and reactive(On demand) and Hybrid protocols. The effort has been made on the comparative study of Reactive, Proactive and Hybrid routing protocols has been presented in the form of table. There are various limitations in different routing protocols and it is difficult to choose routing protocol for different situations as there is adjustments between various protocols. There are various challenges that need to be met, so these networks are going to have widespread use in the future.

International Journal of Advanced Technology & Engineering Research (IJATER) A Study of Congestion Aware Adaptive Routing Protocols in MANET First A. Ms. Harshada Pingale, Research associate; Second B. Ms. Ashwini Rakshe, Research

Ad-hoc networks are useful for providing communication support where no fixed infrastructure exists and movement of communicating parties is allowed. Mobile ad-hoc network shows unexpected behaviour with multiple data streams under heavy traffic load when it is send to common destination. Congestion is one of the most important restrictions of wire- less ad-hoc networks. Because of congestion the problems like long delay, high overhead and low throughput occurred. To overcome these problems in certain degree many congestions aware and congestion adaptive routing protocols are proposed. These protocols can greatly improve the network performance. In this paper, we present a survey of congestion aware routing protocols for mobile network.

This paper emphasised on Traffic Monitoring, Traffic Control & route maintenance activity.

In today's era of wireless mobile adhoc network, congestion is the main cause because of which the performance of wire-less adhoc network gets reduces. In order to building the promising features for adhoc connections, the congestion aware routing protocols will play vital role. So, here on this paper we have studied congestion aware routing protocols in details which will help to relive the influence caused by congestion review of routing protocols for mobile ad hoc networks Mehran Abolhasana**,** Tadeusz Wysocki a, MANETs employ the traditional TCP/IP structure to provide end-to-end communication between nodes. However, due to their mobility and the limited resource in wireless networks, each layer in the TCP/IP model require redefinition or modifications to function efficiently in MANETs. One interesting research area in MANET is routing. Routing in the MANETs is a challenging task and has received a tremendous amount of attention from researches. This has led to development of many different routing protocols for MANETs, and each author of each proposed protocol argues that the strategy proposed provides an improvement over a number of different strategies considered in the literature for a given network scenario. Therefore, it is quite difficult to determine which protocols may perform best under a number of different network scenarios, such as increasing node density and traffic. In this paper, we provide an overview of a wide range of routing protocols proposed in the literature. We also provide a performance comparison of all routing protocols and suggest which protocols may perform best in large networks.

In this paper we have discussed the three categories of unicast routing protocols (in which some may have multicast capability). The global routing protocols, which are derived mainly from the traditional link state or distance vector algorithm, maintain network connectivity proactively, and the on demand (re-active) routing protocols determine routes when they are needed. The hybrid routing protocols is the combination of both reactive and proactive properties by maintaining intra-zone information proactively and inter-zone information reactively.

By looking at performance metrics and characteristics of all categories of routing protocols, a number of conclusions can be decided for each category. In global routing flat addressing can be simple to implement, however it may not scale very well for large networks

3. PROPOSED WORK AND RESULT

In this thesis, AODV was changed to get ideal execution. Two changes were proposed:

- Using the RET as a metric while picking a course.
- Calculating the RET/lifetime for each course, and putting away it in the steering table for that timeframe.

Impressive Today, the scientific efforts are looking for a smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments. For any cryptographic, there is an analogue for Elliptic Curve. One of these systems is Diffie-Hellman key exchange system. This paper proposed methods to encrypt and decrypt the message, by using the Diffie–Hellman Exchanging key which is a secrete point in the proposed methods (M1) and (M2**).**

Our proposed method will be tested under NS-3.20 on Ubuntu 15.04 system with JavaScript:

We describe the improvement of existing Elliptic Curve using Digital Signature and Verification Algorithms for an elliptic curve E defined over a field F = ttF (q). Here q is either a large prime or a large power of 2. Let r be a large prime divisor of the order of E and let tt∈ E be a point of order r. Let s be the private key and W = stt the public key. Denote by f the message representative to be signed (the message or hash of message).

Signature Algorithm:

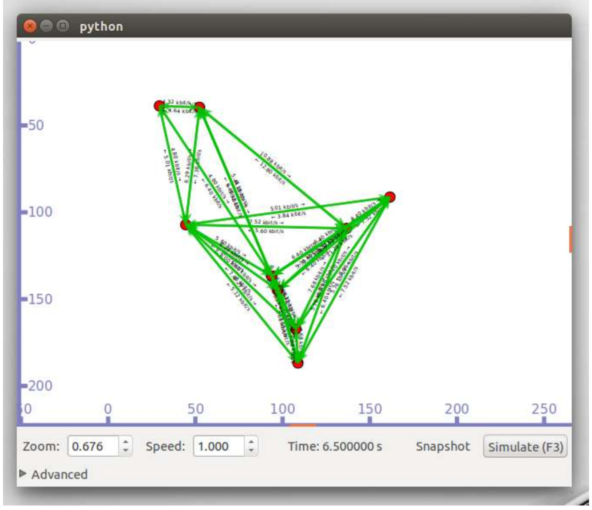
1. Generate a random integer u ∈ [1, .., r − 1] and set V = utt. Write V = (xV, yV).
2. Compute an integer c ≡ xV (mod r). If c = 0 go back to step 1.
3. Compute the integer d = u−1(f + sc) (mod r). If d = 0 go back to step 1.

Output the signature pair (c, d).

Verification Algorithm:

1. If c or d is not in the range 1..r − 1 output invalid and stop.
2. Compute integers h = d−1 (mod r), h1 = fh (mod r), and h2 = ch (mod r)
3. Compute the elliptic curve point P = h1tt + h2W . If P = O, output invalid and stop, else P = (xP, yP)
4. Compute an integer cr ≡ xP (mod r)
5. If cr = c output valid, else output invalid.

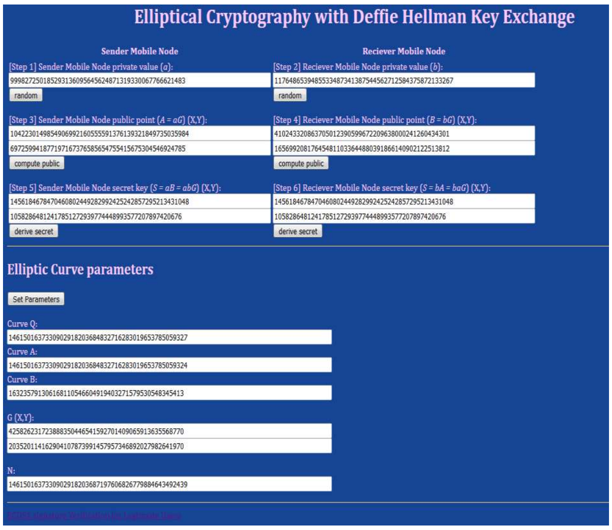
(a) This represent simulation between mobile nodes and topology created during communication and x and y axis's indicate simulation area in meters and in this zoom facility available and speed indicate simulation speed and simulation time shows total time required for simulation and green lines indicate links reacted during simulation between mobile nodes (indicated in RED color) with speedinkbps.



Zoom: 0.676 Speed: 1.000 Time: 6.500000 s

Figure 2: Simulation between Mobile Nodes and Topology created during Communication

(a) This represent communication between mobile nodes after simulation for securing communication using ECCDH key exchange mechanism.



[Step 1] Sender Mobile Node private value (a): 999827250185293136095645624871319330067766621483

[Step 2] Reciever Mobile Node private value (b): 1176486539485533487341387544562712584375872133267

[Step 3] Sender Mobile Node public point ($A = aG$) (X,Y):
1042230149854906992160555591376139321849735035984
697259941877197167376585654755415675304546924785

[Step 4] Reciever Mobile Node public point ($B = bG$) (X,Y):
410243320863705012390599672209638000241260434301
165699208176454811033644880391866140902122513812

[Step 5] Sender Mobile Node secret key ($S = aB = abG$) (X,Y):
1456184678470460802449282992425242857295213431048
10582864812417851272939774448993577207897420676

[Step 6] Reciever Mobile Node secret key ($S = bA = baG$) (X,Y):
1456184678470460802449282992425242857295213431048
10582864812417851272939774448993577207897420676

Elliptic Curve parameters

Curve Q:
1461501637330902918203684832716283019653785059327

Curve A:
1461501637330902918203684832716283019653785059324

Curve B:
163235791306168110546604919403271579530548345413

G (X,Y):
425826231723888350446541592701409065913635568770
203520114162904107873991457957346892027982641970

N:
1461501637330902918203687197606826779884643492439

Figure 3: Elliptical Cryptography with Deffie Hallman Key Exchange

4. CONCLUSION

From the aftereffects of the recreations, it can be inferred that for CBR activity, improved AODV is more helpful at higher portability situations 'encounters marginally higher control overhead than AODV with secure communication using ECCDH. Be that as it may, the change in the parcel conveyance proportion, the mean end-to-end delay, and the throughput exceed the potential hindrances of expanded control overhead.

One street for future investigation is test the AODV completely against more parameters and for various sorts of development. Direct of the transmission control tradition would moreover be a fascinating district of examination. Advance changes would should be made to make this tradition most suitable for quick airborne frameworks. One technique for achieving this is use the development of cross-layer participation between various tradition layers. Assist ponder in this course would be amazingly profitable.

REFERENCES:

[1] H. Yangcheng, G. Kannan, S. Bhatti, S.N. Merchant, and U.B. Desai, "Route dynamics for shortest path first routing in mobile ad hoc networks," in *Proc. Wireless Telecommunications Symposium*, 2017, pp. 24-26,236-242.

[2] T. Wei and G.Wei, "A path reliable routing protocol in mobile ad hoc networks," in*Proc. 4thInt. Conf. on Mobile Ad hoc and Sensor Networks*, 2016, pp. 203-207.

[3] N. Sadagopan, F. Bai, B. Krishnamachari, and A. Helmy, "Paths: Analysis of path duration statistics and their impact on reactive MANET routing protocols," in *Proc. MobiHoc*, 2016.

[4] Y. Han, R. J. La, and A. M. Makowski, "Distribution of path durations in mobile adhoc networks—Palm's theorem at work," in *Proc. of the ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Systems*, 2017.

[5] R. J. La and Y. Han, "Distribution of path durations in mobile ad hoc networks and path selection," *IEEE/ ACM Transactions on Networking*, vol. 15, no. 5,2015.

[6] S. De, A. Caruso, T. Chaira, and S. Chessa, "Bounds on hop distance in greedy routing approach in wireless ad hoc networks," *Int. J. Wireless and Mobile Computing*, vol. 1, no. 2, Feb. 2015, pp. 131-140.

[7] M. Srinivasan, "Analysis of path duration in mobile ad hoc networks," M. Science thesis, Dept. of Electrical and Computer Engineering, Wichita State University, Wichita, Kansas, 2016.

[8] Z. Cheng and W. B. Heinzelman, "Exploring long lifetime routing (llr) in adhoc networks," in *Proc. of the 7th ACM Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2014.