ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

ADVANCED ELLIPTIC CURVE CRYPTOGRAPHY ENCRYPTTION SCHEME for NETWORK-CODED MOBILE AD HOC NETWORKS

S.Kiruthika (P.G Scholar), Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, India.
kiruthicse93@gmail.com

C.Selvarathi(Assistant Professor), Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, India.
selvarathi.cse@mkce.ac.in

ABSTRACT— Security is being a major threat in information sharing through networks. For making the information secure in the existing system P-coding, lightweight encryption scheme is used. AES encryption algorithm is used for encryption/ decryption in this scheme. Permutation encryption is done in the sender side and no changes can be done in the intermediate nodes. Decoding can be done can be done using the key at destination. Since it is a lightweight scheme, security cannot be provided for long time and energy utilization increases in each node. In this paper, a new scheme called Elliptic Curve Cryptography (ECC) is designed in which a key will be attached based on the location of the sender and the receiver. If any of the intermediate node or the attackers try to find the key used for encryption and decryption they will not be in the location used for generating the key so the key cannot be hacked. Now the data will be sent secretly to the destination and the data can be taken by the receiver without any loss or corruption. Simulation results, compared with existing work, show that ECC achieves better security and energy efficiency.

Index Terms—Mobile ad hoc networks, energy saving, network coding, lightweight encryption, Elliptic Curve Cryptography

I. INTRODUCTION

In Mobile Ad Hoc Network, the network can be changed without depending on the infrastructure. The devices that are connected in this network can change their location based on their needs. MANET is capable of operating by them self. Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to correspond without any fixed infrastructure and predetermined association of available links. A MANET is an infrastructure less network, because the mobile nodes in the network energetically set up paths with themselves to transmit packets. Application of MANET includes battlefield applications, search and rescue operations in addition to civilian applications such as e-commerce, business, vehicular services and shopping and other networking applications. Since MANET can be implemented rapidly with moderately low cost, it becomes an attractive option for profitable uses in sensor system applications or virtual classrooms.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

The communication frequency needed for MANET is just the radio frequency (30 MHz – 5 GHz). A well known example for the devices that are connected in MANET is laptops. Laptops can change their network infrastructure in which they are connected based on their needs. MANET consists of various types such as Vehicular Ad Hoc Networks (VANETs), Smart Phone Ad Hoc Networks (SPANs), military MANETs. The main challenges of MANET are Absence of infrastructure, Wireless links among nodes, Limited physical security, Lack of centralized monitoring, safety, Routing, Quality of Services (QoS) Reliability, Energy Utilization and Security.

Energy consumption is one of the most vital performance metrics for wireless ad hoc networks, it directly relate to the operational life span of the networks. Mobile elements have to rely on finite source of energy. While battery technology is improving over time still the need for power consumption will not diminish. This point will have a harmful effect on the operation time as it have connection quality and bandwidth. In the Wireless Ad-hoc Networks, battery replacement may not be possible. So energy consumption concerned, should try to preserve energy while maintaining high connectivity.

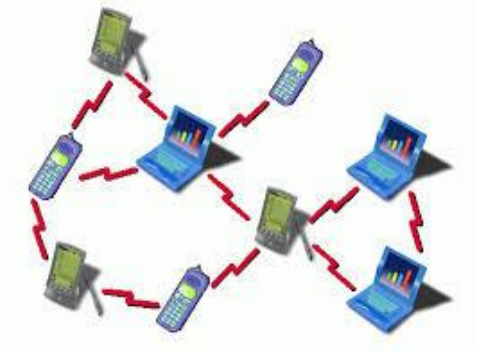

Fig.1. Example of Mobile Ad Hoc Network

Each node should depends on small low-capacity batteries as energy sources, and cannot expect replacement while operating in hostile and isolated regions.

For Wireless Ad hoc Networks, energy depletion and reduction is the primary factor in connectivity degradation and span of operational lifetime. Overall performance becomes highly dependent on the power efficiency of the algorithm. Power consumption is one of the most important performance metrics for wireless ad hoc networks for the reason that it directly relates to the operational lifetime of the network.

Most research efforts are focused on performance comparisons and trade-off studies among various low energy routing and self-organization protocols. As a result, very little has been revealed about the relationship between energy consumption and non-protocol parameters such as node density, network coverage area, and transceiver power characteristics.

Emphasis energy consumption not only because that it is the key problem in the research of Wireless Ad-hoc Networks, but also, find that Energy consumption problem also affects the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

routing protocols and the QoS of the whole networks. Let assume that each source randomly selects one of the possible routes and asks the intermediate nodes on the route to relay traffic.

Energy is a valuable resource, intermediate nodes may not wish to consume their energy to hold the source's traffic. This is called "Selfish" of the node. However, if every node behaves 'Selfish' and decline to cooperate, network throughput may be significantly reduced. Also, there are many works have done to solve the energy consumption problem. Though, unfortunately, little practical information is available about the energy consumption performance of wireless ad hoc network interfaces and device specifications do not provide data in a form that is helpful to protocol developers which again prove that the Wireless Ad Hoc Networks cannot be put into practice. Further, can hold position that the Wireless Ad Hoc Networks are a fundamentally flawed architecture.

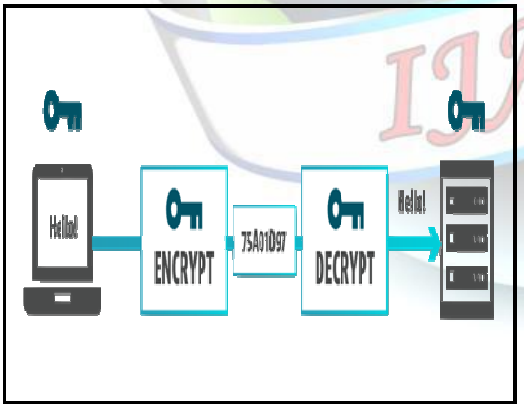

Fig.2.Encryption and Decryption

Security is also an significant issue for Mobile ad hoc Network. Basic security requirements of MANET are Confidentiality, Integrity, Non repudiation and availability, Authentication. Security is measured as an important requirement due to the reason that many upcoming applications demand high security communications. Key management is the core section of the security infrastructure. Christo Ananth et al. [5] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. But in network coding, there are algorithms available to merge the messages which are sent to the same destination. The destination node can use the same algorithm for getting the original information.

Network coding is useful for various networks like file sharing peer-to-peer networks, multicast streaming networks, storage networks, messaging network, mesh networks and other similar networks where the same information has to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

be sent to more destination nodes. From this we can understand the main aim of network coding is to allow and encourage intermediate nodes to mix the data. The efficiency of large networks can be increased by using network coding.

The remaining of the paper is organized as follows. Section II describes some related work about various network coding schemes. Section III presents the working procedure of P-Coding. In Section IV, we proposed the Elliptic Curve Cryptography which has high security. Section V concludes the paper.

II. RELATED WORK

Yunnan Wu et al "Minimum-Energy Multicast in Mobile Ad Hoc Networks Using Network Coding"

An important application domain of network coding is MANETs. By having random fusion packets self-coordinate multiple path, network coding offers built-in error protection and topology changes due to joins, leaves, node or link failures or congestion; by employing a flood-type delivery, network coding can be implemented in a distributed fashion simply, whereas the formation and maintenance of distribution trees incurs notable signaling overhead given the energetic environment. These properties afford network coding potentially useful for unicasting and multicasting in MANETs. The advantage of network coding in efficiently using network resources more specifically the energy consumption in a MANET. The demonstrates that network coding can guide to solutions that are economic in using network resources than routing solutions. we show that, under a layered replica of wireless networks, the minimum energy-per-bit for multicasting can be found in polynomial span via a linear program. The linear program outputs an optimal allocation of bit-rate resources on the links; using the owed link bit rates, the minimum energy-per-bit can be attained by performing network coding, but not routing .

Li (Erran) Li Ramachandran Ramjee et al "Network Coding-Based Broadcast in Mobile Ad hoc Networks"

Broadcast operation is often used both to disseminate data to all nodes and for finding unicast routes in armed ad-hoc networks. Therefore, broadcast efficiency is very important. Due to the potentially dynamic nature of ad hoc networks, restricted algorithms are much more robust and effective with less maintenance overhead. In this system, we show how to incorporate network coding into a non-coding based localized algorithm called PDP for improving broadcast efficiency. We illustrate our approach in the context of PDP, our CODEB coding algorithm can potentially be useful to other non-coding based schemes. The algorithm tries to optimize the coding gains given a set of resident packets and the subset of packets each dependent receives. We design two coding algorithms: an XOR-based simple coding algorithm and a Reed-Solomon-based coding algorithm. The first trouble is NP-hard. We outline a simple greedy algorithm. The second can be solved professionally and optimally using Reed-Solomon codes. Our widespread simulation shows that non-coding based method sends as much as 60% more packets with compact packet delivery ratio. For future work, we intend to explore more on the dependability issue and implement CODEB in a genuine 802.11-based

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

mobile ad hoc testbed in order to thoroughly evaluate its efficacy.

Nachiketh R et al "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols IEEE transactions on mobile computing"

Demonstrate that security processing can have a significant collision on battery life. Addressing the battery gap in secure connections requires that we first analyze and recognize the energy consumption characteristics of safety protocols and cryptographic algorithms. This system presents a comprehensive energy measurement and study of the most popular transport-layer safety protocol used in the Internet, the Secure Sockets Layer or Transport Layer Security protocol. To our knowledge, this is the first widespread energy analysis of the energy necessities of SSL/TLS. The energy analysis is performed by executing secure information transactions on a battery-powered system (a Compaq iPAQ PDA), measuring the current pinched from the power supply and calculating the power consumed during the span intervals in which the security protocol or its essential cryptographic algorithms are executed. Our results can be used to explore the collision of various parameters at the procedure and cryptographic algorithm levels, on overall power consumption for secure data transactions. Based on our study, we discuss various opportunities for energy-efficient security protocols.

Kapil Bhattad et al "Weakly Secure Network Coding"

A special case in the new model. Give an information theoretic definition for significant information which is suited for many practical systems. Then give a constructive proof to show that it is possible to multicast without instructive any meaningful information and without any loss in rate when the number of autonomous messages available to the eavesdropper is less than the multicast capacity of the network. Then study the robustness of the security scheme against an eavesdropper who is able to procure some side information. Show that it is possible to multicast at the multicast capacity using a secure network code that is maximally protected against guessing. I.e. if the eavesdropper has access to k independent messages and the multicast capacity is h then it is achievable to construct a rate h multicast code such that for the first h – k – 1 guesses the eavesdropper gets at most one representation per guess but with h – k guesses he recovers all h symbols. Then consider the case of computationally limited eavesdropper. With the use of one way functions, show that the system can be made protected against a computationally partial eavesdropper without any loss in rate when the number of independent messages accessible to the eavesdropper is less than the multicast capacity. Compute bounds on the probability that a random code is not protected and show that the probability can b e made arbitrarily close to zero by increasing the field size.

Russell et al "Making the Most of Two Heuristics: Breaking Transposition Ciphers with Ants Matthew"

Cryptography has had a long and colorful history. The earliest schemes, now termed the classical

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

ciphers, were intended to be carried out with pen and system rather than by electronics. Many were transpositions: algorithms which sort the order of letters in a message. Classical cryptography became outdated after the advent of computers; more complex ciphers are used and older ciphers wrecked with greater ease. Nonetheless, modern analogues of classical schemes can be found as mechanism of larger ciphers. In scrupulous, some iterated block ciphers, such as the Data Encryption Standard, incorporate transpositions to offer diffusion. The cryptanalyst's tactic when presented with a transposition was to develop particular statistical features of the cipher text, as well as to rely upon intuition, luck and trial-and error, to find the accurate decryption. As this was sometimes too slow a process, mechanized aids were used as early as World War II by which frequencies of letter pairs (known as bigrams) were automatically examined in order to narrow down the space of realistic keys. The outstanding few keys could then be checked exhaustively by hand to recover the plaintext. Consider the prospect of fully automating this procedure. A straightforward implementation turns out due to random difference in the bigram heuristic. We quantify which cryptograms are hard for this algorithm. It shown that the pheromone feedback mechanism of an Ant Colony System is capable of decrypting a wider variety of messages and overcoming some random variation.

III. EXISTING SYSTEM

P-coding. This is a lightweight scheme designed to prevent network-coded MANETs from eavesdroppers. In this the symbols are randomly mixed in each coded packets using permutation encryption so that the eavesdroppers may find it difficult to locate coding vectors for decoding the packets. Network coding allow intermediate node to mix incoming data flows in order to reduce energy consumption as well as transmission time. Network coding is implemented with performing x-or operation on packet data. Without network coding the router just store and forwards the received messages to intended node. When Alice and Bob want to exchange data 4 transmissions are required This requires only 3 transmissions. If energy consumed by encryption/decryption is not considered ¼ energy can be saved.

We concentrate on two factors 1) lightweight scheme in computation by leveraging network coding, which reduces energy utilization. 2) analysis on the weak security provided by network coding. We show that network coding is not when coding vectors are randomly chosen over a large finite field. The basic idea is to perform permutation encryption on coded messages. The proposed scheme based on permutation encryption.

Definition 1. Let m = [m1, m2, …mn] be a sequence of symbols, k be the permutation of length n. The permutation encryption function is Ek(m) = [mk(1),mk(2),……mk(n)]. The permutation decryption function is Dk(Ek(m)) = m. K is the PEF key. To utilize the permutation encryption in real applications

1) The plaintext must be protected; otherwise it is easy to deduce the key k by correlating it with the cipher text.
2) The encryption key should be chosen randomly, which is intuitively necessary for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

PEFs to be effective. The idea of proposed scheme is to mix symbols of the messages and corresponding GEVs and reorder together after performing permutation encryptions on coded messages. PEF key shared by symmetric key which is established by key distribution centre. Algorithm: key generation The proposed scheme based on three stages Encoding by source, Recoding by intermediate node, and Decoding by sink.

According to our assumption the source and sinks can share a PEF key *k* at bootstrap stage of P-coding by KDC which is responsible for symmetric key exchange.

Source encoding: first the messages are prefixed with their corresponding unit vectors and then they are combined with randomly chosen LEVs. Then the permutation encryption is performed to get cipher text.

Intermediate recording: Using PEF we rearrange the symbols and GEVs. The intermediate node does not have any knowledge about the key used so that the source message cannot be reconstructed. But since the permutation encryptions are exchangeable with linear combinations, this stage can be performed on the encrypted messages. This makes it efficient and no extra effort is needed.

Sink decoding: Once the message is being received then it can be decrypted by performing permutation decryption

Advantages of p-coding are as follows, Compression of coded message using compression algorithm is done on coded message. Eavesdroppers cannot achieve the meaningful data from the compressed data. Due to compression the transmission time and cost is bargain. Enhanced P-Coding does not cause any space slide thus is lightweight. Large volume of information can be transferred securely with less energy with using LZW compression algorithm.

IV. PROPOSED SYSTEM

Elliptic curve cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile and wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations, as well as memory and bandwidth savings. An ECC operates over points on an elliptic curve. The way that the elliptic curve operations are defined is what gives ECC its higher security at smaller key sizes. An elliptic curve is defined in a standard, two dimensional (x,y) Cartesian coordinate system by an equation of the form:

$$Y^2=x^3+ax+b \pmod p$$

The graph, when plotted with the above equation, turns out to be gently looping lines of various forms. In ECC, the key is not shared because the public key as well as private keys are in form of points. The working of ECC is explained in the following steps:

Let the finite field be GF (p) and the elliptic curve be E. Choose randomly a base point (x,y) lying on the elliptic curve. Code the plaintext into an elliptic curve point (xm , ym) is applied by splitting the message 'm'. Split the message 'm' into 'n' shares of secret m_t 1<= t<=n Convert each

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

shares mt to a point on EC. With at least‘t’ shares of p, if possible to recover message.

Each user selects a private key ‘n’ and compute his/her public key p=n(x,y) For example, user A’s private key is nA and the public key is pA=nA(x,y) For anyone to encrypt and send the message point (xm,ym) to user A, he/she needs to choose a random integer k and generate the cipher text,cm={k(m,n),(xm,ym)+kpA The cipher text pair of points uses A’s public key, where only user A can decrypt the plain text using his/her private key.

Consider a network abstraction where the source and intermediate nodes have access to the identifiers of the sinks. This way, our schemes can be easily adapted to the many classes of networks that share this characteristic, in particular networks with no centralized knowledge of the network topology or of the encoding functions. It is worth pointing out that network coding has been proposed at several different layers of the protocol stack, for instance addresses the network layer, whereas focus on the application layer. Cross-layer protocols appear. Further assume that the source and sink nodes share symmetric keys to encrypt data as needed. Several mechanisms can be used for the exchange of shared keys, such as an offline mechanism for pre-distribution of keys, an authentication protocol such as Kerberos or a Public Key Infrastructure.

ECC Working Procedure

Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA, Rabin, and El Gamal.

Every user has a public and a private key.

- Public key is used for encryption/signature verification.
- Private Key is used for decryption/signature generation.

Elliptic curves are used as an extension to other current cryptosystems.

- Elliptic Curve Diffie-Hellman Key Exchange
- Elliptic Curve Digital Signature Algorithm
- The central part of any cryptosystem involving elliptic curves is the elliptic group.
- All public-key cryptosystems have some underlying mathematical operation.
- RSA has exponentiation (raising the message or cipher text to the public or private values)
- ECC has point multiplication (repeated addition of two points).

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

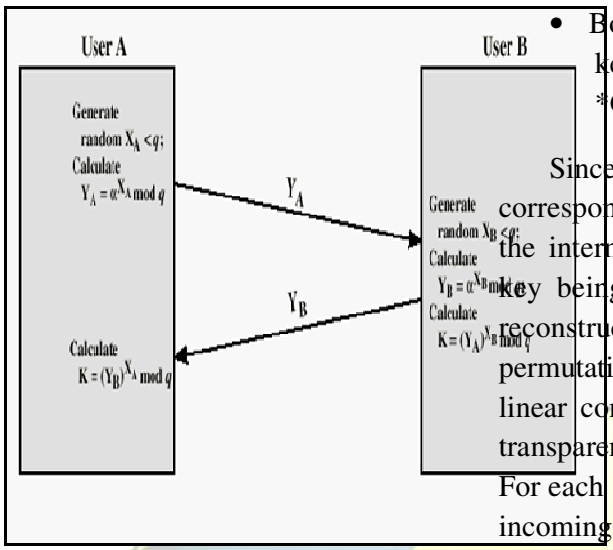

Fig. 3. Encryption/Decryption

Key generation method -- Agree on the following (public):

- Curve parameters (a, b)
- The modulus p
- Base point G (on the curve)
- Pick a random integer *n* as private key
- Calculate public key *P* = n*G Diffie-Hellman (DH) Key Exchange

Encryption/Decryption

- Alice represents her text or data to send as a point P_m
- Alice sends Bob a pair of points: C_m= {k*G, P_m + k*P_B},where k= randomly chosen integer
- Bob decrypts the message using his private key: $P_m + k*P - n_B (k*G) = P_m + k(n_B *G) - n_B (k*G) = \mathbf{P_m}$

Since the symbols of messages and corresponding GEVs are rearranged via PEF, and the intermediate nodes have no knowledge of the key being used, it is rather difficult for them to reconstruct source messages. On the other hand, as permutation encryptions are exchangeable with linear combinations, intermediate recoding can be transparently performed on the encrypted messages. For each sink node, on receiving a message from its incoming link, it decrypts the message by performing permutation decryption on it. Finally, the source messages can be recovered by applying Gaussian eliminations.

If the PEF key does not leak in any generation, the security level of enhanced scheme is as high as that of the P-Coding scheme. When single generation failure occurs, the enhanced scheme can provide two appealing properties.

Security After the compromise of security in current generation, the security level in following ones will be strong enough to resist further attacks. It shows this by evaluating the computational complexity for the adversary to guess the next PEF key based on the current one. First, it should locate the start point of key perturbing operation, which has O (n) different choices.

Then it should fix the correct sequence of the perturbed section of PEF key, which has O (m) different choices. It is fair to assume that these choices are equally possible, according to the randomness property of permutation encryption in P-Coding. Finally, the adversary should decode the messages by performing, which requires O (h3)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

multiplication operations. Thus, the computational complexity in terms of multiplication is O (n m! h^3), which can be made sufficiently large by choosing m properly. Recovery is the PEF key is perturbed randomly and incrementally, it will become more and more irrelevant to its original value with the iterations of generations. Thus, even if the current key is disclosed, its randomness to the adversary will gradually recover after several generations.

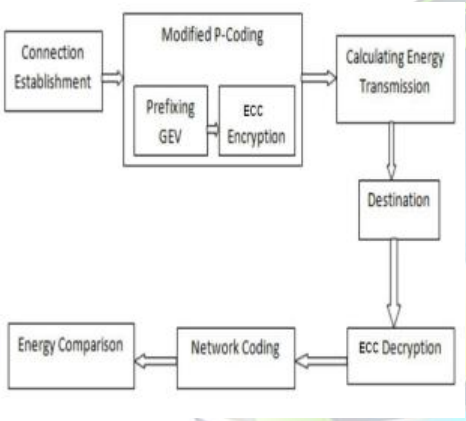

Fig.4.Working procedure of ECC

Fig.4 shows the step by step actions that are done in the proposed system along with the comparison stages.

V. CONCLUSION

This system solve the difficulty of power reduction in MANETs based on the method of network coding. Existing system established so as to network coding can reduce energy consumption by means of less transmission in MANETs. Future P-Coding, an encryption system on top of network coding, to further reduce energy consumption in MANETs by cutting the security charge. P-Coding exploits the built-in security possessions of network coding, and uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. Elliptic Curve Cryptography in terms of the performance parameters like key generation time, Encryption time, Decryption time and communication cost, is efficient in computation, and incurs less energy consumption for encryptions/decryptions. Future work includes extending the application of P-Coding to advance encryption concept such as ECC-TC.

REFERENCES

[1] *Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen , "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Network" IEEE Trans. on Parallel and Distributed Systems, vol. 25, no. 9, Sep 2014*

[2] *L. Li, R. Ramjee, M. Buddhikot, and S.Miller, ''Network Coding-Based Broadcast in Mobile Ad-Hoc Networks,'' in Proc. IEEE INFOCOM, 2007, pp. 1739-1747.*

[3] *N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, ''A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,'' IEEE Trans. Mobile Comput., vol. 5, no. 2, pp. 128-143, Feb. 2006*

[4] *K. Bhattad and K.R. Narayanan, ''Weakly Secure Network Coding,'' in Proc. NetCod, Riva del Garda, Italy, Apr. 2005..*

[5] *Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[6] *Y. Wu, P. Chou, and S. Kung, ''Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding,'' IEEE Trans. Commun., vol. 53, no. 11, pp. 1906-1918, Nov. 2005.*

[7] *Z. Haas, J. Halpern, and L. Li, "Gossip-based ad hoc routing," in Proceedings of IEEE INFOCOM, June 2002.*

[8] *K. M. Alzoubi, P.-J.Wan, and O. Frieder, "New distributed algorithm for connected dominating set in wireless ad hoc networks," in Proceedings of HICSS, 2002.*

[9] *H. Lim and C. Kim, "Flooding in wireless ad hoc networks," Computer Communications Journal, 2001.*

[10] *W. Lou and J.Wu, "On reducing broadcast redundancy in ad hoc wireless networks," IEEE Transactions on Mobile Computing, 2002*

[11] *R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul.2000.*

[12] *P. A. Chou, Y.Wu, and K. Jain, "Practical network coding," in Proc. 41st Allerton Conf. Commun., Control, Computing, Oct. 2003, [CD-ROM].*

[13] *T. Ho, R. Koetter,M.Médard, M. Effros, J. Shi, and D. Karger, "Toward a random operation of networks," IEEE Trans. Inf. Theory, submitted for publication.*

[14] *T. Ho, M. Médard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," in Proc. 41st Allerton Conf. Commun., Control, Computing, Oct. 2003, [CD-ROM].*

[15] *T. Ho, R. Koetter,M.Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in Proc. Int. Symp. Inf.Theory, 2003, p. 442..*