Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Ring-based Fully Homomorphic Encryption Key Management Schema for Multicast Security in Mobile Ad Hoc Networks

[1]S. Sugantha Priya*, [2]R. Marutha Veni
[1]Research Scholar, [2]Asst Professor
[1, 2] Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

Abstract— In Mobile Ad Hoc Networks (MANET), because of moveable nodes, congregation mobility and changing of infrastructure, given that protected communications is a huge challenge. Frequently cryptography methods have been proposed to solve this problem in MANET. In cryptographic techniques, asymmetric cryptography is extensively second-hand because of its factors like verification, reliability, and privacy and straightforwardness designed for key distribution. At the same time multicasting routing in MANET during forward and backward secrecy communication results high packet drop ratio and less security. Since simultaneously changing key values in the MANET causes high message loss, high communication overhead, high energy consumption and high end-to-end delay. Therefore efficient multicast key management method is required to solve the problem of existing cryptographic methods in the key management technique. In this paper presents a Ring-Based Fully Homomorphic Encryption (RBFHE) based key management technique for dynamic multicast group management with mobility managements to solve the problems verification, reliability, and privacy with the purpose of multihop communication. The most important idea is to comprise group members dynamically contribute to the safety of the multicast group, consequently reducing the message loss, communication overhead, energy consumption and end-to-end delay. During this process key value is generated between the nodes in the MANET for multicast communication and satisfies less message loss, less communication overhead, less energy consumption and less end-to-end delay. The allocation of keys in a legitimate manner is a hard task in MANET which is overcome in this work. Through simulation experimentation results shows that the proposed RBFHE approach attains less packet drop rate and improves the data privacy throughout multicasting process.

Keywords— Reliability, Security, Multicasting, Mobile Ad Hoc Networks (MANET), Ring-Based Fully Homomorphic Encryption (RBFHE).

I. INTRODUCTION

A group of wireless communication nodes executing self configuration and self determinant in a self-motivated mode designed for development of network exclusive of predetermined infrastructure is called as mobile ad hoc network (MANET) [1]. It describes the collection of wireless heterogeneous mobile nodes with the intention of carry out communication through each other multihop paths devoid of predetermined infrastructure [2]. The key aspire of MANETs is toward expand the mobility criteria in self-governing, movable, and wireless domain. The nodes in MANET carry out as together hosts as well as routers designed for sending the packet toward every other [3]. Throughout ad hoc routing, each node in the network is acceptable toward determine its multihop path by means of the network toward some other node [1]. The uses of the MANET comprise of military battlefields, disaster investigates, and set free locations, and consequently forward which necessitate quick operation and dynamic reconfiguration. At this time the members formulate use of mobile devices are designed for sharing the information [1]. The development of broadcasting the packets toward a group of hosts acknowledged through a single destination address is named as multicasting [1]. During this process message is shared from source to destination or sender to multiple receivers, which reduces the packet loss with high resources overloading [4] and energy consumption [5]. During multicast communication, routing is performed for efficient communication. In literature several numbers of the routing schemas such as tree based, mesh based, stateless multicast and hybrid approaches [6-7] is introduced for efficient multicast communication. On the other hand, group key management designed for huge and dynamic groups in is hard problem since of the scalability, security below the limits of nodes' obtainable resources and changeable mobility [8]. But some of the key management methods is not suitable for MANET, since of the distinctiveness and the challenges of such environments [9].

Several numbers of investigations is proposed in the recent work for the development of the key management methods in MANET without consideration of the central node. Without consideration of central node, Diffie-Hellman (DH) protocol [10-11] is proposed in recent work. DH key management methods with the intention of together the sender and recipient of a message contain key pairs. By means of mingling single private key and the additional party's public key, together parties are able to calculate the similar shared secret key number. The generated secret number is changed into the cryptographic key, known as two-party DH protocol and enlarged to n--party communication. In [12], proposed a Digital Signature Algorithm (DSA) [12] with the intention of together forward secrecy and key innovation be able to be guaranteed, at the same time as preserving privacy.

© 2015, IJARCSSE All Rights Reserved

In a protected multicast group communication, every member possesses a key to determine and decrypt the multicast communication. In multicast group communication, the process of sending and distribution of the keys in the group members requires a rekeying process. On the other hand, all through frequent membership modulation, key management requirements numerous exchanges as per piece time designed for upholding forward and backward secrecies .In general secure multicasting communication is divided into two ways such as centralized and distributed scheme. The Group Controller (GC) carryout group key management and applied to centralized scheme. In this paper presents a Ring-Based Fully Homomorphic Encryption (RBFHE) based key management technique for dynamic multicast group management with mobility managements to solve the problems verification, reliability, and privacy with the purpose of multihop communication. The most important idea is to comprise group members dynamically contribute to the safety of the multicast group, consequently reducing the message loss, communication overhead, energy consumption and end-to-end delay.

II. BACKGROUND STUDY

In [13] introduced a new clustering based key management method for MANET. The proposed clustering based key management protocol is performed based on the clustering procedure. In this process the MANET is separated into several numbers of clusters relying on their similarity among nodes in the network. For secure communication, private and public keys are generated by means of each cluster head. The clustering based key management protocol is adaptive because of their battery power and dynamic changes in the network environment. This clustering based key management is performed based on the scalable key management schema affords confined communications among the nodes of the MANET.

Wang et al [14] proposed a new Hierarchical Key Management Scheme (HKMS) designed for protected group communications in MANETs. To perform secure communication, packets transmitted from source to destination are encrypted twice. HKMS is performed based on group maintenance in regulate toward compact by means of changes in the topology of a MANET. Experimentation analysis is carryout between the proposed HKMS and existing key management conventional methods it demonstrate that the proposed HKMS have secure group communication than the other schemas.

Bechler et al [15] suggested a new clustering based key management method for MANET. They proposed clustering based key management schema is performed based on the dispersed certification ability. In this process the MANET is separated into several numbers of clusters and cluster head node is selected for each cluster. These cluster head nodes generate key values to each cluster members and share between them. Furthermore the generated key value is also used for verification. In every cluster, accurately single well-known node–the cluster head (CH)–is accountable designed for creating and categorize the cluster. Clustering is moreover second-hand in some of the routing protocols designed for MANET. Decentralization is achieved via the use of threshold cryptography and a network secret with the intention of disseminated over a numeral of nodes.

Jason et al [16] proposed a new scalable key management and clustering scheme designed for protected group communications in MANET. In the proposed work scalable key management and clustering scheme, scalable problem is solved via the use of group communication in each subgroup, and addition separates those subgroups into hierarchies. The level of hierarchy in this schema is known as tier or layer. The hierarchical layer is in the order of Key creation, allocation, and actual information transmissions. Distributed Efficient Clustering Approach (DECA) introduces new clustering methods to perform group communication and experimentation results shows that the proposed DECA have achieves high energy-efficient when compare to existing methods. The proposed DECA method is particularly scalable and well-organized, affords more safety guarantees, and is discriminating, adaptive and strong.

In [17] proposed a new secure group key management scheme designed for hierarchical MANET and large-scale wireless ad hoc networks. A multilevel safety representation and a decentralized group key management communications are performed. This group key management scheme approach decreases communication overhead and increases high throughput by solving single failure problem. Bouassida and Bouali [18] proposed a new Group Key Management Protocols (GKMP) for MANET. In this work the experimentation results of the proposed GKMP is compared to four existing group key protocols such as GKMP with Adhoc Networks (GKMPAN) , Distributed Multicast Group Security Architecture (DMGSA), BALADE, and Hierarchical group key management protocol (Hi-GDH). From this analysis says that the GKMPAN is illustration for centralized approach. DMGSA approach is applied for distributed key management scheme. BALADE protocol and Hi-GDH is applied for decentralized approach.

III. PROPOSED RING-BASED FULLY HOMOMORPHIC ENCRYPTION (RBFHE) FOR KEY MANAGEMENT METHODOLOGY

Key management is a fundamental part of any safe communication. The majority of protected communication protocols depending on key management cryptographic methods. In the initial stage of the work nodes in the MANET is categorized into strong and weak nodes depending on their stability index. The stability index of the each node is determined based on their link accessibility (LQ) and mobility. The strong and weak nodes are categorized depending on their calculation of Link Quality (LQ) in MANET. From this calculation multicast tree is constructed to each node.

Estimating Received Signal Strength. In this research work uses a Friis free space propagation model to determine the Received Signal Strength (RSS) value and determined by the use of the following formula [19]:

$$RSS = \alpha . \theta . S_{tx}$$

© 2015, IJARCSSE All Rights Reserved

where α is a constant value and determined based on the wavelength and the antennas. θ is the channel gain. S_{tx} is transmitter power value. RSS be able to be determined in terms of the dB and dBm (dB milliWatts) and specified using the following formula

$$\mathrm{RSS} = 10\log_{10}\alpha[\mathrm{dB}].\theta.\mathrm{S_{tx}}[\mathrm{dBm}]$$

Link Quality: Link Quality (LQ) is determined via the ratio of the total number of bits in error ($\mathrm{b_{error}}$)to the total number of bits received ($\mathrm{b_{rx}}$) [20]:

$$\mathrm{LQ} = \frac{\mathrm{b_{rx}}}{\mathrm{b_{error}}}$$

Stability Index: Stability index ($\mathrm{SI_{ij}}$) is determined designed for a link to a neighbor relying on the RSS, and link quality [20]. $\mathrm{SI_{ij}}$ is a link among node i and node j is determined as follows:

$$\mathrm{SI_{ij}} = \frac{\mathrm{RSS}}{\mathrm{LQ}}$$

Evaluation of Reputation of Nodes: Regard as nodes i and j. The satisfaction index (P_{ij}) designed for node i regarding node j is determined as follows

$$\mathrm{P_{ij}} = \mathrm{f(i,j)} - \mathrm{e(i,j)}$$

where $f(i, j)$ is the proportion of packets initiated beginning i with the intention of forwarded by means of node j over the total number of packets accessible to node j. (i, j) is the percentage of packets with the purpose of expired greater than the total number of packets accessible to node j. Thus, $\mathrm{P_{ij}}$ be able to be measured as the shortest reputation of node j:

$$\mathrm{Rep_{ij}} = \mathrm{Rep_{ij-pr}} * \mathrm{W_{hist}} + \mathrm{P_{ij}}(1 - \mathrm{W_{hist}})$$

where $\mathrm{Rep_{ij-pr}}$ is defined as the reputation value from node i to node j before determining the satisfaction index. $\mathrm{W_{hist}}$ is a constant with the purpose of reproduce the level of self-confidence with the purpose of node i to neighbor j. The reputation index $\mathrm{REP_{ij}}$ is regularize by means of the following equation,

$$\mathrm{REP_{ij}} = \frac{\mathrm{REP_{ij}}}{\max\limits_{\mathrm{t}}(\mathrm{REP_{ij}})}$$

$\max_t$ is defined as the maximum observation of REP_{ij} over time.

Multicast Tree Construction: The multicast tree is created for weak and strong nodes with two major phases,

Phase 1: Every $\mathrm{N_{wi}}$ sends a child request message (CREQ) in the direction of each prearranged strong neighbor (N_{sj}) in NT:

$$N_{wi} \xrightarrow{CREQ} N_{sj}$$

Leading receiving the CREQ message, N_{sj} sends a child reply message (CREP) in the direction of N_{wi}:

$$N_{wi} \xrightarrow{CREP} N_{sj}$$

Every N_{wi} upon receiving CREP joins by way of N_{sj} as child nodes and individual N_{sj} develop into the parent node. Thus, designed for each weak node, there is at least a strong parent.

Phase 2: In the second phase tree is created and maintained via the use of the periodic "JOIN TREE" messages.

Secure Multicast Communication. If any nodes in the MANET need to communicate and transmit multicast data communication source to destination D in a protected method by using the following steps. In this work secret key is created for each node in the tree by the use of ring element. The scheme, packets transmitted from source to destination during multicast communication is represented as $\mathrm{p_i}$ and$\varphi(\mathrm{n,h})$. The most important structure is the ring R. Let'd' be a positive integer value to generate the key value and key is determined via the use of the ring function as $\mathrm{R} = \mathrm{Z[N_i]}/(\phi_{\mathrm{d}}(\mathrm{N_i}))$ as the ring of polynomials by means of integer coefficients modulo the d-th cyclotomic polynomial $\phi_{\mathrm{d}}(\mathrm{N_i}) \epsilon\, \mathrm{Z[N_i]}$ .The degree of ϕ_{d} is $\mathrm{n} = \varphi(\mathrm{d})$ where φ is Euler's totient function designed for key generation of each node $\mathrm{N_i}$

The elements of R with the intention of number of nodes $\mathrm{N_i}$ be able to be distinctively represented by means of all polynomials in $\mathrm{Z[N_i]}$of degree less than n. Arithmetic in R is arithmetic modulo $\phi_{\mathrm{d}}(\mathrm{N_i})$ which is implicit at whatever time write down terms in R . The arbitary coefficient with the intention of belongs to the packet in R

$$\mathrm{a} = \sum_{\mathrm{i}=0}^{\mathrm{n}-1} \mathrm{a_i}\,\mathrm{N_i} \in \mathrm{R} \quad ||\mathrm{a}||_\infty = \max_{\mathrm{i}}\{|\mathrm{a_i}|\}$$

Where $\mathrm{a_i} \in \mathrm{Z}$ vector coefficients and decide maximum packets based encryption information by means of $\mathbb{R}^{\mathrm{n}}$ to determine the size of elements in R. When reproduce two elements $\mathrm{g, h} \in \mathrm{R}$, by means of respect in the direction of the individual norms of g and h. The maximal norm expansion that can occur,

$\delta = \sup\left\{1 \middle| \frac{|\mathrm{g.h}||_\infty}{||\mathrm{g}||_\infty||\mathrm{h}||_\infty}\right\}$; $\mathrm{g, h} \in \mathrm{R}$ this is a ring constant.

Let χ be a probability distribution on R with the purpose of samples little elements $\mathrm{a} \leftarrow \chi$ by means of high likelihood .

Ring-Based Fully Homomorphic Encryption (RBFHE) scheme is parameterized by means of a modulus q , 1 < t < q. private key are the elements of $\mathrm{R} = \mathrm{Z[N_i]}/(\phi_{\mathrm{d}}(\mathrm{N_i v})$and public key are the elements of R/tR . Secret keys is created for each nodes in the MANET via the distribution key χ_{key} .

The basic encryption and decryption steps for nodes in the MANET is defined as follows :

© 2015, IJARCSSE All Rights Reserved

Basic: ParamsGen (λ): Specified the security parameter λ, with positive integer 'd' with the intention of determines R, modulo q and t by means of 1 < t < q, and distributions χ_{key} , χ_{err} on R output of decrypted key $(d, q, t, \chi_{key}, \chi_{err})$

Basic .keyGen$(d, q. t, \chi_{key}, \chi_{err})$: Sample of the packets $p' g \leftarrow \chi_{key}$ .Compute inverse $p^{-1} \in R$ of r modulo q and set $h = [tgp^{-1}\varphi(n, h)]_q$.

Output the public and private key pair $(pk, sk) = (h, p, \varphi(n, h)) \in R^2$

Basic. Encrypt (h,m):the message space is Rt/R designed for message $m + tR + \varphi(n, h)$ decide $[m]_t$ as its representative and output the secret key of original packets as

$$c = [[q/t][m]_t + e + hs + \varphi(n, h)]_q \in R$$

The information is defined as

$$m = [[t/q \,.\, [pc]_q]]_t \in R$$

Let q, t, and $\Delta = [q/t]$ be as above and let $SK, N_i, m \in R$. If there exists $v \in R$. Such that $N_i S_c = \Delta[m]_t + v(\text{mod } q)$and $||v||_\infty < (\Delta - N_{i_t}(q))/2$ then basic.Decrpt(sk,c)= $[m]_t$ under the secret key s .

Of course, for any known c, s and m, there always exists a $v \in R$ such that $sk_c = \Delta[m]_t + v(\text{mod } q)$.

Known $m \in R$, a public key $h = [tgrs^{-1}\varphi(n, h)]_q$ with secret key $sk = [1 + tsk']_q, sk', g \leftarrow \chi_{key}$ and let $c = \text{Basic. Encrypt } (h, m)$.

RBFHE.Parametergen (λ) : Given the security parameter λ output of the encrypted packet using $(d, q, t, \chi_{key}, \chi_{err}, w)$ where $(d, q, t, \chi_{key}, \chi_{err}) \leftarrow \text{BasicParamgen}(\lambda)$ and w>1 is integer

RBFHE. keygen$(d, q, t, \chi_{key}, \chi_{err}, w)$ compute $h, sk \leftarrow \text{Basic. Keygen}(d, q, t, \chi_{key}, \chi_{err})$ sample $e, s \leftarrow \chi_{err}^{\ell_{w,q}^3}$ calculate

$$\gamma = [sk^{-1}P_{w,q}\left(D_{w,q}(s) \otimes D_{w,q}(rs)\right) + e + h.s]_q \in R^{\ell_{w,q}^3}$$

RBFHE. encrypt$(pk, sk, evk) = (h, sk, \gamma)$

RBFHE. encrypt(pk, m) to encrypt $m \in R$

RBFHE. Decrypt(sk, c) to output the message encrypt $m \leftarrow \text{Basic. Decrypt}(sk, c) \in R$

RBFHE. KeySwitch$(\tilde{c}_{multi}), evk)$: output$[\langle D_{w,q}(\tilde{c}_{multi}), evk\rangle]_q \in R$.

RBFHE. add(C_1, C_2): calculate the addition of C_1, C_2 as $C_{add} = [C_1 + C_2]_q$

RBFHE. multi(C_1, C_2, evk) Compute

$\tilde{c}_{multi} = \left[\left[\frac{t}{q} P_{w,q}(C_1) \otimes P_{w,q}(C_2)\right]\right]_q \in R^{t_{w,q}^2}$ and

output $c_{multi} = \text{RBFHE. multi}(\tilde{c}_{multi}, evk)$

RBFHE. multi(C_1, C_2, evk) compute

$$\tilde{c}_{multi} = \left[\left[\frac{t}{q} P_{w,q}(C_1) \otimes P_{w,q}(C_2)\right]\right]_q \in R^{t_{w,q}^2}$$

$evk = [rs^{-1}P_{w,q}\left(D_{w,q}(rs) \otimes D_{w,q}(rs)\right) + e + h.s]_q$

output by RBFHE. Keygen where $e, s \leftarrow \chi_{err}^{-w,q}$ are vectors of polynomials sampled beginning the error allocation χ_{err} and [.]q is useful toward every coefficient of the vector. In conclusion, the generated subgroup sequence accomplishes the source and it calculates the new group key designed for the group. Once, the new-group key is created by means of the source, it unicasts it to the members strongly.

IV. SIMULATION RESULTS

The proposed RBFHE and existing MBKM, ECGK is measured under varied number of receivers and varied number of movable nodes.

Simulation Model and Parameters: To examine the experimentation results of the proposed RBFHE and existing MBKM, ECGK methods is implemented via the use of NS2 [21]. In the NS2 simulation model, the channel capacity values of mobile nodes is pre-specified to 2Mbps. Make use of the distributed coordination function (DCF) of IEEE 802.11 designed for wireless LANs as the MAC layer protocol. Designed for multicasting, second-hand Multicast AODV (MAODV) [22] routing protocol. Simulations results are conducted under the area of 1500 meter × 1500 meter region between 50 seconds simulation time intervals. During this simulation process make assume that all nodes in MANET are movable with the same average speed. Each and every one node has the equal transmission range of 250 meters. In NS2 simulation model, the speed wide-ranging from 5 to 25m/s and results were measured. In this NS2 simulation model, consider together the node capture and insider attacks. In node capture attack, a malicious attacker appropriates the credentials and generates secret keys from the legitimate nodes. An insider attacker is a malicious legitimate group member which might warm false trust relations and injects false trust exposure. It might moreover inject packets n the network toward concern communications and use the network resources.

TABLE 1: SIMULATION PARAMETERS

Number of receiver nodes	10,20,30,40,50
Area size	1500 x 1500

© 2015, IJARCSSE All Rights Reserved

Mac	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Rate	250 kB
Mobility model	Random way point
Speed	5,10,15,20 and 25

Performance Metrics: Compare the results of the proposed RBFHE schema, existing Mobility Based Key Management Technique (MBKM) [23] and Efficient Clustering scheme for Group Key management (ECGK) [24]. The performance results of these schemas are measured under the following metrics.

Average Packet Delivery Ratio (PDR) is the ratio of the total number of packets received effectively and the total number of packets sent.

Overhead is defined as the controls overhead (in terms of packets) transpire during keying and rekeying operations.

Packet Drop ratio is defined as the total number of packets dropped at each receiver during packet transmission.

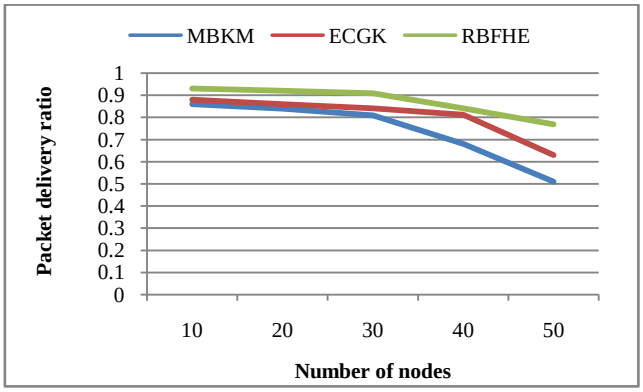

Figure 1. Comparison of packet delivery ratio vs methods

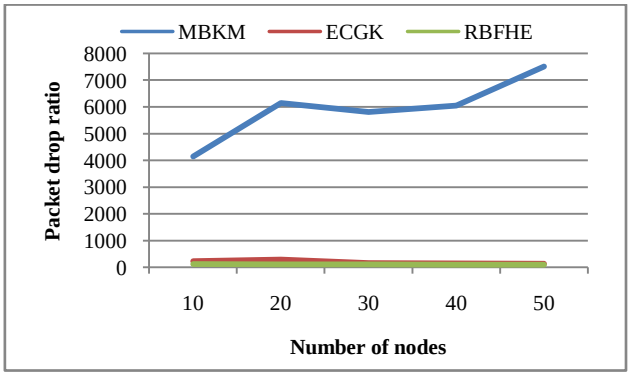

Figure 2. Comparison of packet drop ratio vs. Methods

In the Figure 1 and 2 shows the experimentation results of the Average Packet Delivery Ratio (PDR) and packet drop of three key management techniques such as RBFHE, MBKM and ECGK, respectively with group key size varied from 10 to 50. From the Figure 1, can see that RBFHE, MBKM and ECGK methods has 43.25 % less packet drop than MBKM technique. Because of this reduced packet drop, the PDR of the proposed MBKM is 4.36 % higher than the ECGK technique.

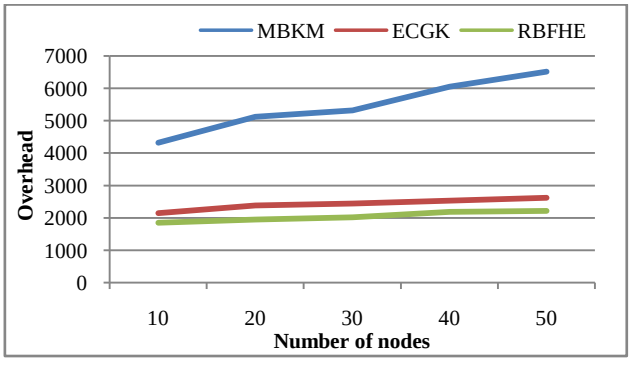

Figure 3. Comparison of overhead vs methods

© 2015, IJARCSSE All Rights Reserved

Figure 3 shows the performance control overhead results of the three key management techniques such as RBFHE, MBKM and ECGK, respectively with group key size varied from 10 to 50. It can be seen that RBFHE, MBKM has lesser overhead than the existing GKMPAN scheme, since the proposed RBFHE doesn't rely on multicast tree structure.

V. CONCLUSION AND FUTURE WORK

Security of group communication is one of the most important key issues in the MANET. Since the secure group communication need to satisfy the following constraints such as accessibility, privacy, honesty, verification, permission and non-repudiation. In recent work several numbers of security methods and schemas have been proposed in the recent work to solve this problem for MANET. Key management is an essential characteristic of the safety of MANET, and it is still an unsolvable problem for many applications. In this paper new mobility based key management schema is presented for multicast safety in MANET. In the initial stage of the work nodes in the MANET is categorized into strong and weak nodes depending on their stability index. The stability index of the each node is determined based on their link accessibility and mobility. Then multicast tree is created for every weak node in MANET. When some node needs to broadcast a multicast communication to destination, Ring-Based Fully Homomorphic Encryption (RBFHE) based key management technique is proposed. The rekeying operation is performed occasionally by means of the initiator node which is selected between the strong nodes relying on the reputation index. The rekeying interval is pre-specified relying on the node category. RBFHE technique method minimizes the packet overhead and end to end delay while minimization of the number of rekeying operation. By NS2 simulation model, simulation results demonstrate that the proposed RBFHE achieves less packet drop rate, high packet delivery ratio and improves the information privacy.

REFERENCES

[1] Junhai, L., Liu, X., & Danxia, Y., "Research onmulticast routing protocols for mobile Ad-hoc networks," *Computer Networks*, vol. 52, no. 5, pp. 988–997, 2008.

[2] Striki, M. &Baras, J. S., "Key distribution protocols for secure multicast communication survivable in MANETs," *In Proceedings of the IEEE Military Communications Conference (MILCOM '03),* Boston,Mass, USA, October 2003.

[3] Rajan, C. & Shanthi, N. S., "Misbehaving attack mitigation technique for multicast security in mobile ad hoc networks (MANET)," *Journal of Theoretical and Applied Information Technology*, vol. 48, no. 3, pp. 1349–1357, 2013.

[4] Srinivasan, R., Vaidehi, V., Rajaraman, R., Kanagaraj, S., Chidambaram, R. Kalimuthu,& Dharmaraj, R., "Secure group key management scheme for multicast networks," International Journal of Network Security, vol. 10, no. 3, pp. 205–209, 2010.

[5] Lazos, L. & Poovendran, R., "Power proximity based key management for securemulticast in Ad hoc networks," Wireless Networks, vol. 13, no. 1, pp. 127–148, 2007.

[6] Kalaidasan, R., Hemamalini, V., & Babu, A. K. , 'SORB: secure on demand resilient to byzantine multicast routing in multihop wireless networks', *In ISCET 2010: Proceedings of International Symposium on Computer Engineering and Technology* , pp. 131-141,2010.

[7] Deepalakshmi, P., & Radhakrishnan, S., "An ant colony based multi objective approach to source-initiated QoS multicasting method for ad hoc networks," *Int. J. Advance. Soft Comput. Appl*, vol.3, no.2,2011.

[8] R. A. and K. C. Shet, "Hierarchical approach for key management in mobile ad hoc networks," *International Journal of Computer Science and Information Security (IJCSIS),* vol. 5, no. 1, pp. 87–95, 2009.

[9] Bouassida, M.-S., Chrisment, I., & Festor, O., "Group key management in MANETS," *International Journal of Network Security (IJNS),* vol. 6, no. 1, pp. 67–79, 2008.

[10] Diffie , W. & Hellman, M. E., "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644– 654, 1976.

[11] Harn, L., Meht, M., & Wen-Jung, H., "Integrating diffie-hellman key exchange into the digital signature algorithm (dsa)," *Communications Letters,* vol. 8, no. 3, pp. 198–200, 2004.

[12] Phan R. C. W., "Fixing the integrated diffie-hellman-dsa key exchange protocol," *Communications Letters, IEEE*, vol. 9, no. 6, pp. 570–572, 2005.

[13] Maghmoumi, C., Abouaissa, H., Gaber, J., & Lorenz, P. , " A Clustering-Based Scalable Key Management Protocol for Ad Hoc Networks," *Second International Conference on In Communication Theory, Reliability, and Quality of Service,* pp. 42-45, 2009.

[14] Wang, N. C., & Fang, S. Z., " A hierarchical key management scheme for secure group communications in mobile ad hoc networks", *Journal of Systems and Software*, vol.80, no.10, pp.1667-1677,2007.

[15] Bechler, M., Hof, H. J., Kraft, D., Pahlke, E., & Wolf, L. , "A cluster-based security architecture for ad hoc networks", *Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies* ,vol. 4, pp. 2393-2403, 2004.

[16] Li, J. H., Levy, R., Yu, M., & Bhattacharjee, B, "A scalable key management and clustering scheme for ad hoc networks", In *Proceedings of the 1st international conference on Scalable information systems* , pp. 28, 2006.

[17] Huang, D., & Medhi, D. , "A secure group key management scheme for hierarchical mobile ad hoc networks", *Ad Hoc Networks*, vol.6,no.4, pp.560-577,2008.

[18] Bouassida, M. S., & Bouali, M. , "On the performance of group key management protocols in MANETs", *In Joint Conference on Security in Network Architectures and Information Systems (SAR-SSI '07)* ,pp. 275-286, 2207.

© 2015, IJARCSSE All Rights Reserved

[19] Sridhara , V. & Bohacek, S., "Realistic propagation simulation of urban mesh networks," *Computer Networks*, vol. 51, no. 12, pp. 3392–3412, 2007.

[20] Biradar, R., Manvi, S., & Reddy M., "Mesh based multicast routing in MANET: stable link based approach," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 2, pp. 371–380, 2010.

[21] Network Simulator, http://www.isi.edu/nsnam/ns/.

[22] Lin, H.-Y. & Chiang, T.-C., "Efficient key agreements in dynamic multicast height balanced tree for secure multicast communications in Ad Hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, Article ID 382701, 15 pages, 2011.

[23] Bouassida, M. S. & Boali, M., "On the performance of group key management protocols in MANETs," *in Proceedings of the Joint Conference on Security in Network Architectures and Information Systems (SAR-SSI '07),* pp. 275–286, Annecy, France, 2007.

[24] Drira, K., Seba, H., & Kheddouci, H., "ECGK: an efficient clustering scheme for group key management in MANETs," *Computer Communications*, vol. 33, no. 9, pp. 1094–1107, 2010.

© 2015, IJARCSSE All Rights Reserved