International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-1, January, 2019

An Improved Efficient Certificate Less Data Transmission (CL-EKM) In Mobile Ad-Hoc Network

Arya K S[1]
Research Scholar[1].
Nehru Arts & Science College,
Coimbatore, Tamil Nadu-641105

P.K.Manojkumar[2]
Head, Associate Professor[2]
Nehru Arts & Science College,
Coimbatore, Tamil Nadu-641105

Abstract: Wireless Sensor Networks (WSNs) have recently developed as a platform for numerous important surveillance and control applications. In the third phase of this research work, a Hybrid Group based Re-Key Management Scheme (HG-RMS) is proposed for securing the group combination in WSN. The suggested HG-RMS approach uses the Hybrid Energy Efficient Distributed (HEED) protocol for electing the group controller for every group. The generation and distribution of keys to the group controllers is performed using RSA algorithm. By exploiting the key exchange mechanism a secure communication is provided between the users. The forward and backward secrecy is achieved using re-keying phase. When compared to the existing Cluster based Group Key Management (CL-GKM), the energy consumption, privacy level, memory, key accuracy and time consumption of the proposed approach is optimal. In this research work, a certificate less effective key management (CL-EKM) is proposed for securing the group combination in WSN. By exploiting the key exchange mechanism a secure communication is provided between the users. The forward and backward secrecy is achieved using re-keying phase. When compared to the existing Methods, the energy consumption, privacy level, memory, key accuracy and time consumption of the proposed approach is optimal.

Keywords: Diffie Hellman, Key Distribution Centre, Shared Key Derivation, Cipher text, Distributed Key Pre-Distribution Scheme

I. INTRODUCTION

In recent advancement the networking will be implemented with the real time radio technologies in computer industry. For mobile devices there is a need for dynamic switching and self-organizing. A MANET is highly designed with mobile platforms termed as nodes. The node may be moved in any direction and in any speed with formulation. The node in the network needs to operate as a source node and destination node.

Key management is the process of handling the cryptographic keys in a secure manner. It includes key generation, storage, protection, transfer, key usage and key abolishment. Four major concerns of key management are key deployment or pre-distribution, key establishment, node addition and node eviction. The distribution of key is performed prior to communication. The key distribution is a significant issue in wireless sensor network. The center for key distribution is used for the key distribution. The symmetric encryption method is not suited for ad hoc network due to its inefficiency.

Key management is an important factor to enhance secure transmission of data in WSN. The data security is provided by the process of encryption and decryption, in which the keys are shared among the nodes to convert the cipher text to readable form. The existing frameworks use many techniques and protocols to achieve high security.

Digital signatures and secure symmetric key exchange are provided by the RSA asymmetric algorithm as well as either of the SHA-1 or MD5 hash algorithms. The standard PGP software combines several algorithms to implement cryptographic protocols in order to provide cryptographic services for email and file storage. So, digital signatures and message encryption are offered to email clients by means of selected asymmetric, hash algorithms, and symmetric.

The traditional techniques suffered from several issues such as maximum usage of resources, higher cost, more time consumption, communication and computational overheads. Further, they did not achieve a high level of integrity, flexibility, scalability, and confidentiality. To reduce the time consumption and storage overhead, McEliece algorithm is proposed. A hybrid group based re-key management scheme is used to share the keys among the appropriate nodes. The forward and backward secrecy is maintained by dynamic key updates in rekeying phase.

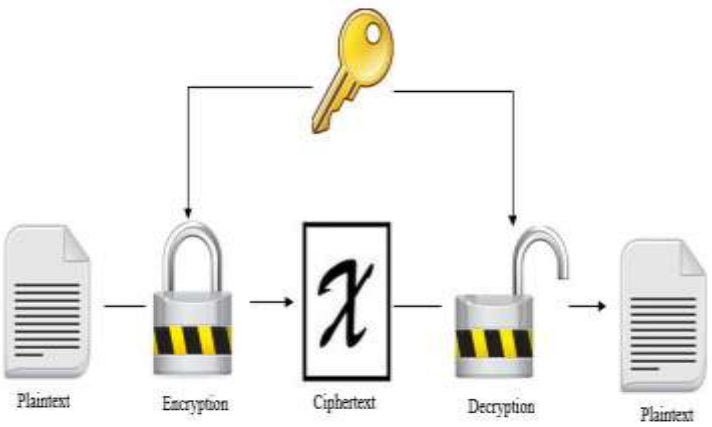


Figure 1 Symmetric cryptographic method

The subsist of the paper is described as. The review in literature is done in Section II. The theoretical design and the phases of the scheme are described in Section III and the experimental results of the computerized system are documented in Section IV. Finally, future work and conclusions are written Section V.

II. LITRATURE REVIEW

The review emphases around representing the past secure routing techniques in remote sensor systems. Thus a system is proposed to structure fluffy classifiers utilizing hereditary calculation that can analyze oddities and other couple of specific interruptions. The premier goal is to create two guidelines. One is for ordinary class and another is for strange class by using a profile informational collection alongside data related with the PC organize at the season of typical activities and furthermore noxious conduct. At long last it indicates couple of arrangements and reports with respect to execution of created fluffy classifiers in distinguishing interruptions.

Olaru and Wehenkel (2003) proposed Zhou et al. [35] proposed a Group Deployment based Improved Key Pre-distribution Scheme (IGDKPS) to improve the security in WSNs. The Blundo method and resolve TD (k,n) method was used to solve the low connectivity and scalability problems. The connectivity rate, flexibility, and resistance were

A portion of the current procedures passed on the issue of isolating the traded off hubs. Be that as it may, every one of these works are appropriate just for static systems as the safe neighbor check is existed with a few impediments which incorporate asset needs, exactness to remote sensor and specially appointed systems.

Sodhro et al. [36] proposed Random Initial and Master Key (RIMK) scheme for establishing and managing the keys in an efficient manner. The traditional methods occupied a large storage space and increased the network complexity.

Thus in portable multi-jump remote systems a method called MOBIWORP is acquainted with soothe from these impediments and to decrease the wormhole assault in systems. This methodology uses the safe focal specialist for worldwide following of area of hubs. And furthermore it utilizes neighborhood checking for finding and isolating the broken hubs locally, hub grabs the information parcels from one position in the system and notwithstanding that if enough data is accumulated at the focal specialist it forces worldwide partition of the traded off hub from the whole system. The effect of introduced MOBIWORP on the information movement is analyzed through NS2 recreation.

A Group key administration system dependent on intermediary re-cryptography fornear space arrange was structured by Wang et al., (2011) The intermediary re-coding construction was utilized in the re-keying process, which illuminates the inconvenience of a solitary level of disappointment. An intermediary re-cryptography allows a semi confided in intermediary to change over a figure content starting with one gathering then onto the next. In this plan a message scrambled by gathering A can be decoded by any of the individuals in gathering B.

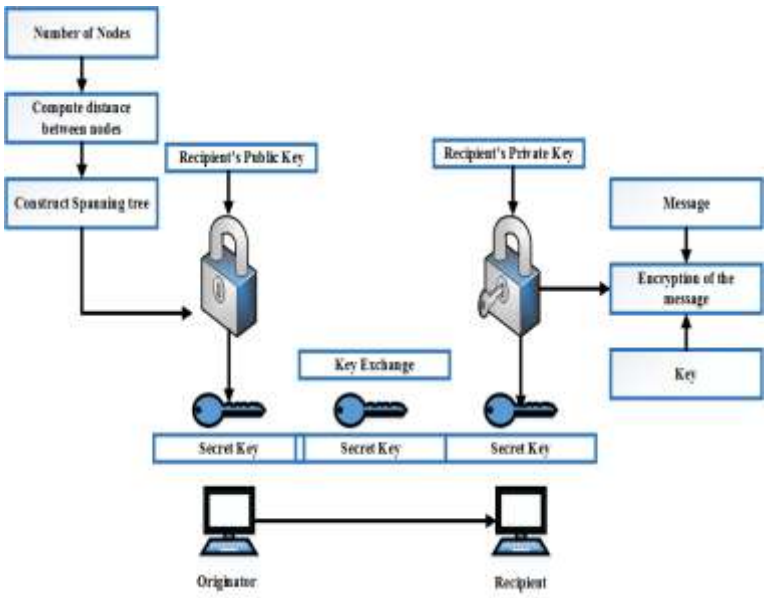


Figure 2 Key management architecture Khalil et al., (2008)

III. PROPOSED SYSTEM

Based on the sensor information, each mobile node in the battle field performs mission critical tasks. Thus, securing the sensitive information is very important for the hostile environment. In most of the group communications, the multicast routing is used for transmitting the message from one sender to multiple users. Security is one of the key issues in multicast group communication. By exploiting multiple keys the security can be enhanced. Further, there is no optimal key management scheme. Proposed system, the security issues are addressed using the Diffie Hellman method based Group Key Management (CL-EKM) scheme. The process involved in the proposed CL-EKM scheme is depicted in Figure 3.

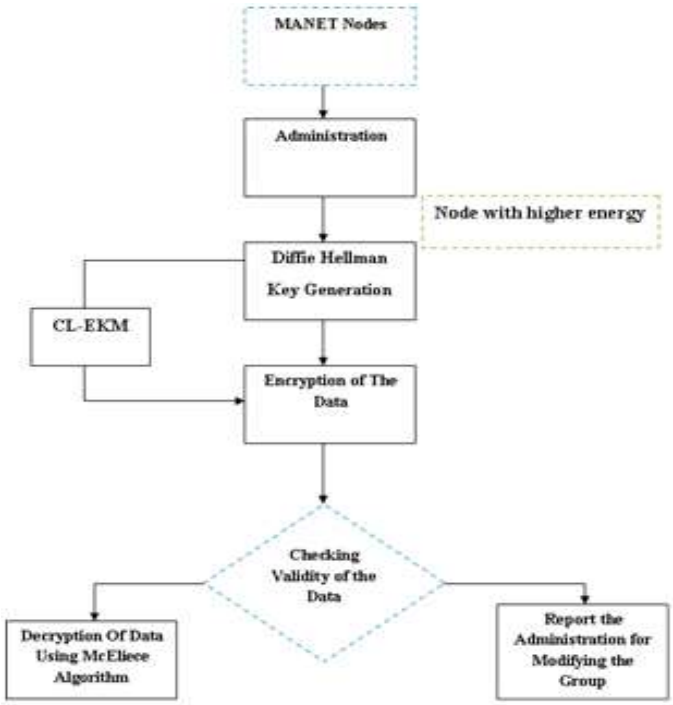


Figure 3 Process involved in the CL-EKM scheme

The overall flow of the proposed Group Key Management (CL-EKM) scheme is shown in the figure 3.2. The key components of the proposed CL-EKM are as follows,

1 Creation of Group Manager (GM)
2 Generate Key (GK)
3 Group key generation
4 Encryption
5 Decryption

CL-EKM, Diffie-Hellman key exchange algorithm is used for generating a shared secret between two people thus provides a secure communication between them. Consider two people say Alice, and Bob wants to share a secret key for using it in the symmetric cipher. During the initial step of the Diffie-Hellman key exchange algorithm, the users Alice and Bob initialize the large prime T, and a nonzero integer n modulo T. The prime number and the non-zero integer values are made public such that the attacker Eve also knows them.

$$A = na(modT)$$

$$B = nb(modT)$$

As Alice, and Bob communicate through the insecure communication channel, the attacker eve monitors the value of A, and B. Based on the secret integers, Alice, and Bob computes the equation (3.8), and (3.9).

$$A' \equiv Ba\ (modT) \qquad (3.3)$$

$$B' \equiv Ab\ (modT) \qquad (3.4)$$

The values A', and B' are same because,

$$A' \equiv Ba \equiv (nb)a \equiv nba \equiv (na)b \equiv A \equiv B'\ (mod\ T)$$

An example for the Diffie Hellman key exchange algorithm is depicted in the figure 3.3.

$$YU \equiv pXU\ mod\ p \qquad (3.6)$$

Where,

P is the prime number

XU denotes the private key of user U

The public key for the user V is estimated as follows,

$$Yv \equiv pXV \ mod \ p \qquad (3.7)$$

$$K \equiv (YV)XU \ mod \ P \qquad (3.8)$$

Where, Yv is the public key of user V. Equation (3.4) describes the computation of the secret key for user V,

$$K \equiv (YU)XV \ mod \ P \qquad (3.9)$$

$$GK = f\,k\ 1k\ 2k\ 3k\ GC \qquad (3.10)$$

The generated keys are distributed among with the group members by using a proactive secret sharing scheme.

$$m \equiv c\ l\ (mod\ n) \qquad (3.12)$$

Once the validity of the authentication is checked, the decryption of the message is performed. Based on the public encryption key *(k, n)*, and private decryption key *(l, n)*, the decryption is performed using the following equation.

IV. RESULT AND DISCUSSION

In this section, the performance of the proposed certificate less effective key management (CL-EKM) scheme by us through network simulator 2 tool simulation platforms. Before conducting the simulations, the initial parameters must be set ahead. The battery initial energy level B0 is set as 2000J . The active power Pc of sensor node and initial active state Ta0 of are set as 16mW and 5h respectively, Tan –min is set as 1h . The sensor node density ρ is one node per 100m2 and the communication radius of sensor node is set as 10m. The energy harvesting power is randomly set during different time periods. Afterwards, we conduct the simulation experiments and the specific results are described as follows table 1describe parameters.

S.NO	PARAMETERS	VALUES
1	Number Of Nodes	10, 20, 30,...,100
2	Simulation Time	200 seconds
3	Area	500*500 meters
4	Number Of Keys	3
5	Key Size	1024 bits
6	File Size	256, 512,..., 2048 bytes

Table 1 parameters and values of CL-EKM MANET

In this section, the performance of the proposed certificate less effective key management (CL-EKM) scheme by us through network simulator 2 tool simulation platforms. Before conducting the simulations, the initial parameters must be set ahead. The battery initial energy level B_0 is set as $2000J$. The active power P_c of sensor node and initial active state T_{a0} of are set as $16mW$ and $5h$ respectively, T_{an} –min is set as $1h$. The sensor node density ρ is one node per $100m2$ and the communication radius of sensor node is set as $10m$. The energy harvesting power is randomly set during different time periods. Afterwards, we conduct the simulation experiments and the specific results are described as follows table 1describe parameters.

Figure 4 A) node generation B) Node compromised and Investigates suspicious Node

We have to state that the number of sensor nodes in each pair is even according to the broadcast message of BS. Once the cluster matrix units are established, two SNs having minimum distance with each other combine to be the SNP. The SNP has equal status but they cannot work at the same time in figure 4. All sensor nodes marked with SN combine into one group (GSN) to perform data collection and transmission, and the others turn to be the other group (GSN'). Each group in any cluster has the ability to monitor the target area that the cluster covers.

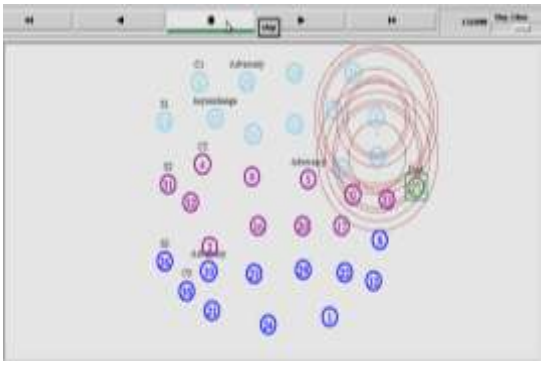
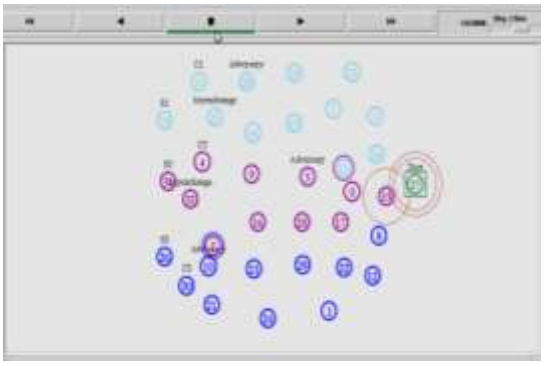
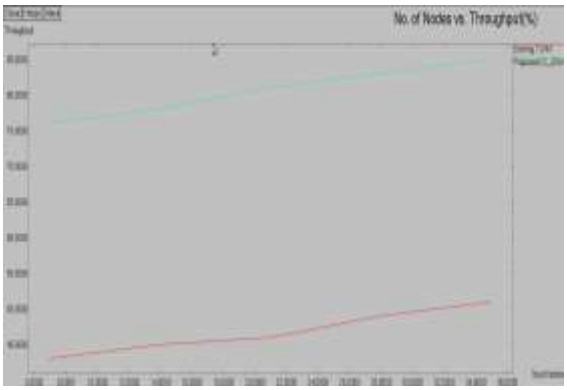
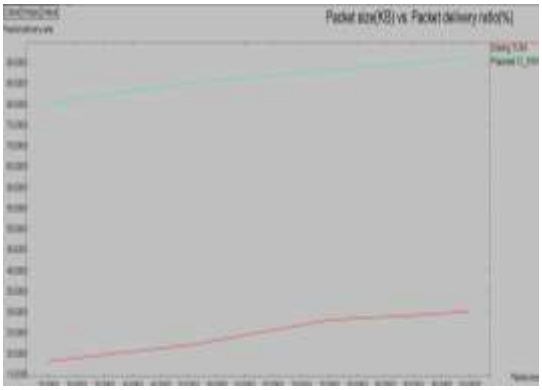
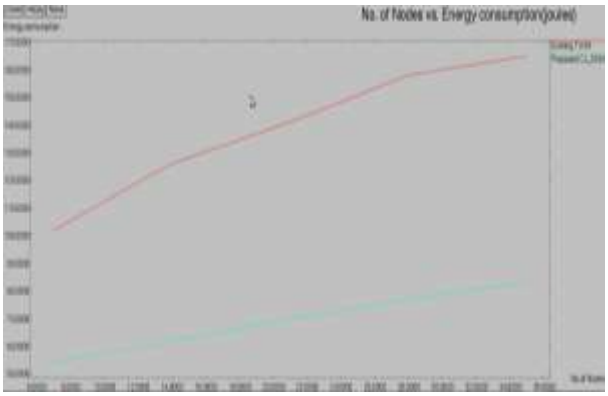



Table 5 a) communication source to designation first path b) second path

To obtain the discrimination of MANET establish the Key Pair Share through the Path as shown in the . in the figure 5 a) communication mode 1 the first path efficiently shares through key from the source 18 to final designation 27 the following manner 18-15- 24 -13 -7- 3- 34 -27 and figure 5 b) Manet communication mode 2 the second path efficiently shares through key from the source 18 to final designation 27 the following manner 31-32-4-9-16-20-17-11-33-27.







6 a) compression result for CL-EKM and TLKM algorithms Number of Node vs throughput. **b)** Pocket size (kb) vs Pocket delivery ratio **c)** number of nodes vs energy consumption

V. CONCLUSION

CL-EKM being promising techniques for the architecture of the MANET, it is important to address its mobility in face of increased delay when considering real-time applications with strict delay requirements. Existing TLKM method consume the long time to solve huge network problem, we introduced the approach of using Certificateless Efficient Key Management System (CL-EKM, The proposed algorithm exploits both the secret key, and group key for encrypting the message. Once the messages are encrypted, the validity of the message is checked. If the message is authentic, the message is decrypted, else, the group member updation process is performed. The comparison of performance for the existing TLKM and the proposed CL-EKM schemes prove that the proposed CL-EKM scheme minimizes the throughput, pocket size (kb), Pocket delivery ratio, number of nodes and energy consumption in joules.

REFERENCES

[1]. J. Gomez and D. Dasgupta, 2011, 'Evolving fuzzy classifiers for intrusion detection', Proceedings of the 2002 IEEE Workshop on the Information Assurance, West Point, NY, USA.

[2]. Olaru, C., & Wehenkel, L. (2003). A complete fuzzy decision tree technique. Fuzzy sets and systems, 138(2), 221-254.

[3]. Zhang, Y., Liu, W., Lou, W., Fang, Y., & Kwon, Y. (2005, May). AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks. In Communications, 2005. ICC 2005. 2005 IEEE International Conference on (Vol. 5, pp. 3515-3519). IEEE.

[4]. Khalil, I., Bagchi, S., & Shroff, N. B. (2008). MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Networks, 6(3), 344-362.

[5]. Eik Loo, C., Yong Ng, M., Leckie, C., & Palaniswami, M. (2006). Intrusion detection for routing attacks in sensor networks. International Journal of Distributed Sensor Networks, 2(4), 313-332.

[6]. Roosta, T., Shieh, S., & Sastry, S. (2006, December). Taxonomy of security attacks in sensor networks and countermeasures. In The first IEEE international conference on system integration and reliability improvements (Vol. 25, p. 94).

[7]. Nishimura, K., & Takahashi, K. (2007, June). A multi-agent routing protocol with congestion control for MANET. In European Conference on Modelling and Simulation (pp. 1-6).

[8]. Khan, S., Mast, N., Loo, K. K., & Silahuddin, A. (2008). Passive security threats and consequences in IEEE 802.11 wireless mesh networks. 2; 3.

[9]. Xu Su, Rajendra V. Boppana, 2008, 'Mitigating Wormhole Attacks using Passive Monitoring in Mobile Ad Hoc Networks', IEEE Conferences, pp.1-5.

[10]. Wang, F., Huang, C., Zhao, J., & Rong, C. (2008, March). IDMTM: A novel intrusion detection mechanism based on trust model for ad hoc networks. In Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on (pp. 978-984). IEEE.

[11]. Nabeel, M., & Bertino, E. (2011, October). Poster: towards attribute based group key management. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 821-824). ACM.

[12]. Sumathy, S., & Kumar, B. U. (2010). Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks. arXiv preprint arXiv:1003.3564.

[13]. Bawa, H., Singh, P., & Kumar, R. (2013). An efficient novel key management scheme for enhancing user authentication in a WSN. International Journal of Computer Network and Information Security, 5(1), 56.

[14]. Zhang, X., & Wang, J. (2015, December). An efficient key management scheme in hierarchical wireless sensor networks. In Computing, Communication and Security (ICCCS), 2015 International Conference on (pp. 1-7). IEEE.

[15]. Cui, B., Wang, Z., Guo, T., Dong, G., & Zhao, B. (2013, September). UBKM: A Usage-Based Key Management Protocol for Distributed Sensor Networks. In 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies (pp. 267-272). IEEE.

[16]. Wang, Z., Du, X., & Sun, Y. (2011, May). Group key management scheme based on proxy re-cryptography for near-space network. In Network Computing and Information Security (NCIS), 2011 International Conference on (Vol. 1, pp. 52-56). IEEE.

[17]. Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (pp. 41-47). ACM.

[18]. Anand, A., & Patel, B. (2012). An overview on intrusion detection system and types of attacks it can detect considering different protocols. International Journal of Advanced Research in Computer Science and Software Engineering, 2(8).

[19]. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on software engineering, (2), 222-232.

[20]. Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1994). A taxonomy of computer program security flaws. ACM Computing Surveys (CSUR), 26(3), 211-254