ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-5, 2019

Key management for the multicast communication in Wireless Network and Cloud: Survey and Discussions

Rajnish Choubey[1], Dr. Shiv Shakti Shrivastava[2], Dr. Santosh K. Gandhi[3]

[1]Ph.d. Research Scholar, Department of CSE, RNTU, Raisen M.P. (India)

[2]Associate Professor, Department of CSE, RNTU, Raisen M.P. (India)

[3]OSD, DTE, Govt. of MP, Bhopal (India)

ABSTRACT

Key management in Wireless Sensor Network (WSN) is a complex task due to its nature of environment, limited resources and open communication channel. In addition, wireless communication poses additional threats to the critical information being sent and received over there. WSN are necessary to be protected from different attacks. But, the major problem to secure WSN is a key distribution after deploying the sensor nodes in specific area. In this paper we present the review for the various key management techniques for the wireless communication especially in the field of multicast communication where one sender shares the key in a group or multiple destinations.

Keywords:- Wireless communication, Mobile ad-hoc network, Key management, Multicasting, Wireless sensor network.

INTRODUCTION

Recent advances in wireless communications technology have enabled seamless connectivity for the large number of wireless devices in today's world. Provision of wireless connectivity to the millions of wireless devices also demands the optimal usage of spectral resources. A few megahertz (MHz) of reserved frequency for wireless communications comes out to be costly.

Communications are divided into three different forms such as unicast, multicast and broadcast. Multicast is an efficient method for transmitting data from a single source to several destinations. Especially, in wireless networks using a broadcast medium, a single transmission can be received by all nodes within a transmission range, which makes it easy to implement the multicast. Therefore, the multicast in wireless networks is expected to pave the way for efficient group communications, by which many group-based applications, such as charged video on demand or video conferencing, can be commercialized [1].

Wireless sensor networks (WSNs) are one of the emerging technologies of this century. Sensor networks are composed of a large number of low power sensor devices. For collection of sensed data from the remote area, it is necessary to install such kind of network in properly secure area. Recent studies in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional tiny devices for use in remote sensing applications. The combination of these factors has improved the capability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and distribution of valuable information gathered in a variety of environments [11].

Key Management is used for secure communication either in case of Symmetric key or asymmetric key algorithms. For the implementation of various security schemes, Key distribution is not typical in WSNs, but constraints such as small memory capacity make centralized keying techniques impossible. Straight pairwise key sharing between every two nodes in a network is not suitable for large growing networks. Efficient security scheme and reliable key distribution must be used between all relevant nodes. Key management scheme using cryptographic function based on symmetric and asymmetric has been becoming effective solution in this regard. There is various ways in which we can classify key management schemes in wsn by considering different benchmarks. Various researchers gave different taxonomies. Key management scheme in wsn can be broadly classified into dynamic and static solutions based on whether rekeying is perform after deployment. In the case of static key management scheme, once sensor nodes are deployed in the desire field and they will not change and administrative keys are generated before deployment. Administrative keys are change periodically or on demand in the case of dynamic key management scheme. Network survivability and scalability are the major advantages of dynamic key management scheme. All the nodes have same capability in the case of homogeneous schemes commonly a flat network model. Based on the encryption, it is classified into symmetric, asymmetric and hybrid key management scheme.

The rest of this paper is organized as follows in the first section we describe an introduction of about the mobile ad-hoc network, vehicular ad-hoc network. In section II we discuss about the wireless communication introduction and wireless communication in vehicular ad-hoc network, In section III we discuss about the literature survey in the vehicular ad-hoc network, In section IV we discuss the about protocol layers or OSI model, finally in section V we conclude the about our paper.

II Mobile Ad-Hoc Network

As this era of electronic age time where security has become essential part of all communications. MANET is one of the prominent examples of wireless communication which are responsible for communication between sender and receiver with full security and as we are well aware, MANET network is one of the diluting connectors in which exchange of data is done in regulated form. MANET web writes structural path to communicate from person to person. In previous years, presentation of the wireless has increased vastly, therefore, one sets new field of request in the span of computer networks and such field concerns mobile ad-hoc network. A MANET is self configuring web of mobile routers related by wireless links. The wireless gesture router is in free random gesture and they code themselves to connected data. These kinds of web work in non existence of each field infrastructure. It is extremely tough to make the use of continuing routing method for web services and it poses assorted trials in safe guarding the protection of the communication as its well known safe guarding protection is easily completed as countless of the demand of web protection fight alongside the demand of the mobile web majorly because of the nature of the mobile mechanism, example low manipulation consumption and low processing load. Mobile Ad-hoc web is a set of wireless nodes that are vibrantly linked and transfer information. Wireless nodes can be confidential computers (desktops/laptops) alongside wireless LAN cards, Confidential Digital Assistants (PDA), or supplementary kinds of wireless or mobile contact devices.

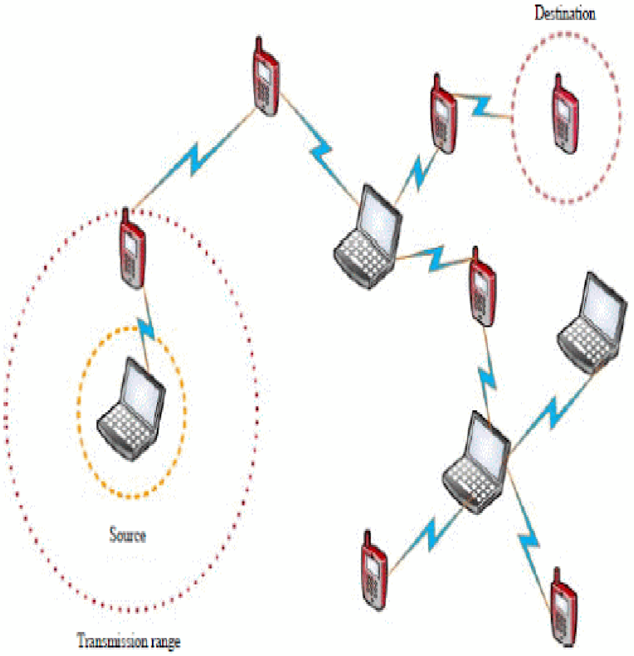

Fig 1: Architecture of MANET.

Current Challenges of MANET The major challenges of MANET to work on their weakness and to make their strength to be more powerful as like security is not safe anymore which is very poor and a part of it the dynamic topology to make more efficient.

Limited Bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition to the realize throughput of wireless ad hoc network after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

Dynamic Topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

Routing Overhead: In wireless networks, nodes often change the location within their network. So, some stale routes generated in the routing table which leads to unnecessary routing overhead.

Packet Losses due to transmission errors: In ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, interference, uni-directional links, and frequent path breaks due to mobility of nodes.

Mobility-Induced route changes: The network topology in ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

Battery Constrained: It Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

Power Awareness: as it well aware MANET network work by batteries that is the biggest challenge of this network so for making more efficient the battery has to be preserved.

Addressing Scheme: The web topology keeps changing vibrantly and hence the addressing scheme utilized is quite significant. A vibrant web topology needs an omnipresent addressing scheme that avoids each duplicate address. In wireless WAN settings, Mobile IP is being used.

Security Threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality was established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

III Related Work

[1] In this paper, they propose a new GKM scheme for multiple multicast groups, called the master-key-encryption-based multiple group key management (MKE-MGKM) scheme. The MKE-MGKM scheme exploits asymmetric keys, i.e., a master key and multiple slave keys, which are generated from the proposed master key encryption (MKE) algorithm and is used for

efficient distribution of the group key. It alleviates the rekeying overhead by using the asymmetry of the master and slave keys, i.e., even if one of the slave keys is updated, the remaining ones can still be unchanged by modifying only the master key. Through numerical analysis and simulations, it is shown that the MKE-MGKM scheme can reduce the storage overhead of a key distribution center (KDC) by 75 percent and the storage overhead of a user by up to 85 percent, and 60 percent of the communication overhead at most, compared to the existing schemes. [2] This paper has proposed the novel resource allocation schemes (hybrid resource management) for EE maximization problem in the emerging scenarios of the wireless networks, i.e., small cell, massive MIMO, massive MIMO HetNets and cell-free. Besides, the necessary constraints of QoS threshold and power budget are guaranteed while the objective EE function in terms of bits/Joule/Hz is optimized. Each of scenario is carefully considered and simulated by numerical results. [3] In this paper author propose a protocol which was based on content-based to take care of some characteristic issues in wireless sensor networks, particularly in correspondence. The protocols based on content are primarily amplified the rate of appropriate message conveyance and limit the energy utilization by utilizing strategies to keep up briefest ways. It passes information by utilizing a platform based on agent, where every sensor can take on its choice separately. This protocol extends the network lifetime. When the nodes gets dead, the system consequently build new route for sending data. Also, this proposed work utilizes Homomorphic encryption for security purpose. Performance evaluations are done using efficiency metrics and it can be utilized for evaluating the lifetime of the system. [4] A method for providing the security of data before storing in cloud as well as reducing storing space was proposed in this research and using key management module, the security of keys and their management were considered. They have proposed a plan in this paper which is very effective and efficient in order to ensure user’s data in cloud storing space. The experiments showed that proposed plan leads to reduce cloud storing space and maintain the Integrity and confidentiality of user’s data. They have also showed that proposed algorithm has a good speed. In case of hacking user’s authentication, user’s data and information can be hacked so as the future researches, a mechanism is recommended to be considered that authentication operation is conducted through a secure protocol and also parallel encryption is recommended to be used for cloud big data which increases the speed of encrypting data and proposed algorithm of AES is capable of parallelism which is absolutely effective for cloud big data. [5] This paper describes the different techniques along with few security challenges, advantages and drawbacks. It also provides the analysis of data security issues and privacy protection affairs related to cloud by preventing data access from unauthorized users, managing sensitive data, providing accuracy and consistency of data stored. To deal with these security problems, this paper also proposes a novel data sharing mechanism that concurrently achieves data confidentiality and fine-grained access control on encrypted data and user revocation by combining ciphertext policy attribute-based encryption and proxy re-encryption. This paper also delivers security for cloud data storage through a proper key management system with multiple key managers using Shamir’s key sharing technique and the policy file encryption is done using Elgamal algorithm for secure data transmission. [6] The proposed work uses multi-group key management protocol for key generation and encryption, and AES algorithm has been used for key decryption. Since the complexity of these algorithms is low, it ensures a high-speed key generation, encryption and decryption thus increasing the efficiency of VANET. Also, the packet drop ratio is greatly reduced due to fast and efficient key management scheme used in the proposed approach. The experimental results show that the use of decentralized key distribution mechanism is able to overcome the bottleneck situation and greatly increases the throughput for the key management system in the proposed approach. [8] in this paper they propose a novel revocation management

scheme by utilizing cryptographic accumulators which not only reduces the space requirements for revocation information but also enables convenient distribution of revocation information to all smart meters. They implemented this one way cryptographic accumulator-based revocation scheme on ns-3 using IEEE 802.11s mesh standard as a model for AMI and demonstrated its superior performance with respect to traditional methods of CRL management through extensive simulations.
[9] In this article, the current state of memristive cryptography is placed in context of lightweight hardware cryptography. The paper provides a brief overview of the traditional hardware lightweight cryptography and cryptanalysis approaches. The contrast for memristive cryptography with respect to traditional approaches is evident through this article, and need to develop a more concrete approach to developing memristive cryptanalysis to test memristive cryptographic approaches is highlighted. [11] In this paper, they identify the some existing schemes of key management in WSNs. Secure key management has been becoming important critical elements when integrating cryptographic functions into a system. An outline of symmetric and asymmetric key cryptography Key infection schemes are discussed in this paper. As a consequence, they analyze the advantages and disadvantages of current secure key management schemes. [12] In this paper, they present a comprehensive survey of WMCRNs. Various multimedia applications supported by CRNs, and various CR based wireless networks are surveyed. They highlight the routing and link layer protocols used for WMCRNs. They cover the quality-of-experience (QoE) design and security requirements for transmitting multimedia content over CRNs. They provide an in depth study of white space, TV white space, and cross-layer designs that have been used for WMCRNs. They also survey the major spectrum sensing approaches used for the communications of bandwidth hungry and time-critical data over CRNs. [13] Security is very essential in the modern electronics world. AES algorithm is further enhanced by incorporating multiple hardware optimization design strategies to achieve ultra low power, high throughput and energy efficient design with multiple levels of security. In this survey, overview is given of perceptual methods of information hiding techniques specifically cryptography was discussed. Familiar encryption techniques, efficient bio-cryptography algorithms and image encryption schemes are also exposed. This approach can also be implemented using different biometric traits like face, voice etc. The paper also gives a concise idea of using efficient hardware architecture techniques and it can be used for further research purposes.

IV Group Key Management Approaches

Moreover, there are two types of cryptography; the first type is symmetric key cryptography that uses one key for encryption and decryption and it is faster to execute like Advanced Encryption Standard (AES). The second type is known asymmetric cryptography or called private key system that use two keys one key for encryption it's called private its secure but the second its public key for decryption like Rivest-Shamir-Adleman algorithm (RSA), Elliptic Curve Cryptography (ECC), and Elliptic Curve Computational Diffie-Hellman (ECCDH) to provide best security [18]. Nowadays, WSNs have attracted significant interest in the engineering community and among researchers. In fact, the wireless channels are not secure. In addition, Due to the depending on the keys to make a connection between the nodes in a radio channel (open environment), these keys are easily prone to attack. Thus, the main challenge in the WSNs is the security of the key distribution that is used for the connection.

Group key management approaches are classified into 3 major categories:

1. **Centralized: O**n this methodology key distribution capability is carried with the aid of a single entity, which governs key generation and distribution whenever needed. Thus, a group key management protocol looks to attentive storage needs, computational force on both client and server sides.

2. **Distributed:** It is based totally on organization signature to make sure privacy in vehicular ad hoc network (VANETs). All the present organization signature schemes are based on a centralized key control wherein the keys are preloaded into the vehicle.

3. **Decentralized**: This approach is a mixture of former approaches (centralized and distributed). An authorized cluster is split to some little subgroups so they create some graded levels. This approach shares the advantage and disadvantage that are expressed in centralized and distributed schemes. Considerately of those reasons, this theme is a lot of enticing for using during this work [6].

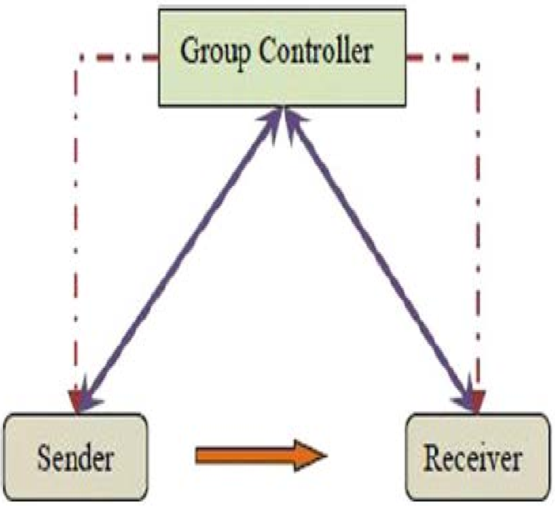

Fig 2: Basic model for group key management.

V Conclusions

The key management has a fundamental role in securing group communications taking place over vast and unprotected networks. It is concerned with the distribution and update of the keying materials whenever any changes occur in the group membership. Wireless mobile environments enable members to move freely within the networks, which causes more difficulty to design efficient and scalable key management protocols. This is partly because both member location dynamic and group membership dynamic must be managed concurrently, which may lead to significant rekeying overhead. This paper presents the various key management scheme reviews in wireless communication and in future we implement the secure and efficient key management scheme in wireless communication to improve the performance of the overall network.

REFERENCES:-

[1] Min-Ho Park, Young-Hoon Park, Han-You Jeong, Seung-Woo Seo, “Key Management for Multiple Multicast Groups in Wireless Networks”, IEEE Transactions on Mobile Computing, Vol. 12, 2013, pp 1712-1723.

[2] Long D. Nguyen, “Resource Allocation for Energy Efficiency in 5G Wireless Networks”, EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 2018, pp 1-7.

[3] S. Veerappan, Dr. R. Vadivel, “Homomorphic Encryption Algorithm Used For Security Enhancement in Wireless Sensor Network Content-Based Routing”, International Journal of Advanced Research in Computer Science, 2018, pp 345=348.

[4] Attar N, Shahin M, “A Proposed Architecture for Data Security in Cloud Storage Space”, Journal of Biostatistics and Biometric Applications, Vol-3, 2018, pp 1-7.

[5] Nidhi Shah, Digvijay Mahida, “Data Security in Cloud Computing : A Comprehensive Survey”, International Conference on Current Research Trends in Engineering and Technology, 2018, pp 434-438.

[6] Shikha Rathore, Jitendra Agrawal, Sanjeev Sharma and Santosh Sahu, “Efficient Decentralized Key Management Approach for Vehicular Ad Hoc Network”, Springer 2019, pp 147-161.

[7] Ramon Agüero, Bernd-Ludwig Wenning, Yasir Zaki, Andreas Timm-Giel, “Architectures,

Protocols and Algorithms for 5G Wireless Networks", Sringer 2017, pp 1-3.

[8] Mumin Cebe, Kemal Akkaya, "Efficient Public-key Revocation Management for Secure Smart Meter Communications using One-way Cryptographic Accumulators", IEEE 2018, pp 1-6.

[9] Alex Pappachen James, "An overview of memristive cryptography", Springer, 2019, pp 2301-2312.

[10] D.I. George Amalarethinam, H.M. Leena, "A Comparative Study on various Symmetric Key Algorithms for enhancing Data Security in Cloud Environment", International Journal of Pure and Applied Mathematics, 2018, pp 85-94.

[11] Usham Robinchandra Singh, Sudipta Roy, "Survey on Key Management Schemes and Cluster based Routing Protocols in Wireless Sensor Network", Proceedings of International Conference on Computational Intelligence & IoT, 2018, pp 576-595.

[12] Muhammad Amjad, Mubashir Husain Rehmani, Shiwen Mao, "Wireless Multimedia Cognitive Radio Networks: A Comprehensive Survey", IEEE 2017, pp 1-49.

[13] Chinnandi Arul Murugan, P. KarthigaiKumar, "Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms", Mobile Networks and Applications, Springer 2018, pp 1-6.

[14] Pranshu Bajpai, Aditya K Sood, Richard Enbody, "A Key-Management-Based Taxonomy for Ransomware", IEEE 2018, pp 1-12.

[15] Shaukat Ali, Azhar Rauf, Naveed Islam, Haleem Farman, Bilal Jan, Murad Khan, Awais Ahmad, "SGKMP: A scalable group key management protocol", Sustainable Cities and Society, Elsevier ltd. 2018, pp 37–42.

[16] Antonio Celesti, Maria Fazio, Antonino Galletta, Lorenzo Carnevale, Jiafu Wanb, Massimo Villari, "An approach for the secure management of hybrid cloud–edge Environments", Future Generation Computer Systems, Elsevier ltd. 2019, pp 1–19.

[17] Mr. T. Vijaykanth Reddy, B. Kalyani, M. Nikitha, M. Rukesh, "Integration of Multi User Key Management with Policy Previlege using ABE in Cloud", International Journal of Engineering Technology Science and Research, Vol-5, 2018, pp 53-58.

[18] Kameran Ali Ameen, " Key Management Distribution Scheme in Wireless Sensor Network Based on Knapsack Algorithm", Kirkuk University Journal /Scientific Studies, Vol-13, 2018, pp 17-33.

[19] J. Vijayalakshmi, K. Prabu, " Approaches of Key Management Schemes for Mobile Ad-Hoc Networks", National Conference on Innovative Research Trends in Computer Science and Technology, 2018, pp 4-9.

[20] Satyajit Sarmah, Shikhar Kumar Sarma, " Dynamic Bandwidth Management in 802.11Wireless LAN", International Journal of Computer Sciences and Engineering, 2018, pp 95-99.