A MODIFIED ENHANCED KEY MANAGEMENT SCHEME FOR WSN

[1]Er. SHIKHA, [2]Er. RAVI KUMAR

[1]Student (M.Tech), Department of C.S.E., Geeta Institute of Management And Technology, Kurukshetra University, Haryana, India

[2]Assistant Prof., Department of C.S.E., Geeta Institute of Management And Technology, Kurukshetra University, Haryana, India

ABSTRACT

Wireless sensor networks (WSNs) consisting of low power, low-cost intelligent devices that have limited IT resources. With an overall growth of WSN applications, security mechanisms are also a big problem on the rise. Many Real world applications have already been deployed and many of them will be based on wireless sensor networks. Examples of these applications include surveillance, health care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring and surveillance. Wireless sensor network security issues have three aspects, key management, authentication, and secure routing. As the features of wireless sensor network node resource are limited, asymmetric key system has been considered unsuitable for wireless sensor networks; after elliptic curve cryptography (ECC) has been proposed, asymmetric key system application in wireless sensor networks has become possible. Compared to the symmetric key system, asymmetric key system has great advantages in terms of management and security keys. In recent years, many scholars have proposed many effective key management schemes based on ECC public key infrastructure. The proposed and implemented work deals with key management which is based on Diffie-Hellman algorithm. This approach avoids the storage requirements for the key and avoids the security risks for the master key or the key derived from the master key. The approach is suitable for any type of wireless sensor network which contribute to the security of Wireless sensor network. The approach makes the pair wise key for the communication and provides the secure and authenticated access to the information exchange between nodes which satisfy the objectives of the work proposed.

I. INTRODUCTION

Advances in wireless communication and electronics have enabled the development of low-cost, low power, multifunctional sensor nodes. These tiny sensor nodes consisting of sensing, data processing, and communication components make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks [1].

These sensors are deployed in harsh environments to collect different types of data such as temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects and other properties [2, 3]. The collected data is then sent to a special node called the base station (BS) either directly or via other sensor nodes. BS is a more powerful device that usually behaves as an interface between the services provided by the sensor nodes (the "data acquisition network") and the users of the network. It can issue control orders to the sensor nodes in order to change their behaviour.

II. RELATED WORK

Tahira Laskar, Debasish Jena, (2012) in the paper "A Survey on Key Management Issues in WSN" stated that security concerns of the sensor nodes becomes more challenging issue since nodes are positioned in adverse environment. Key management have the crucial role for communication in WSNs. The key management system should be substantially secure, robust and efficient for a secure communication protocol. Many key establishment ttechniques have come up to address the tradeoffs between limited memory and security but choosing an effective scheme is debatable.A survey of various key management schemes in WSNs. Choosing a key management scheme depends upon the target application requirements and the resource of the sensor network.

Cristina Alcaraz, Javier Lopez, Rodrigo Roman, Hsiao-Hwa Chen, (2013) in the paper Selecting Key Management Schemes for WSN Applications" stated that Key management in wireless sensor networks (WSN) is an active research topic. Due to the large number of key management schemes (KMS) proposed in the literature, it is not easy for a sensor network designer to know exactly which KMS best fits in a particularWSN application. a comprehensive review on how the application requirements and the properties of various key management schemes influence each other is presneted. Based on this review, it is proved that the KMS plays a critical role in determining the security performance of a WSN network with given application requirements. a method that allows the network designers to select the most suitable KMS for a specific WSN network setting is developed. It also addresses the issues on the current state-of-the-art research on the KMS for homogeneous (i.e. nonhierarchical) networks to provide solutions for establishing link-layer keys in various WSN applications and scenarios.

Seema Verma, Prachi, (2014) in the paper "A Comparative Study of Key Management Protocols for WSN" stated that Increased employment of WSN (Wireless Sensor Network) in real life applications and their hostile and remote locations accelerate demand of security in WSN. Publicly accessible wireless communication channel also makes WSN vulnerable to numerous security attacks. Scarcity of resources acquaints new sort of challenges and difficulties during implementation of effective security mechanisms.It evaluate and compare performance of three different security mechanisms (ECRKS, CKP and AP scheme). ECRKS (Energy-efficient, Connected, Resilient Key pre-distribution Scheme) is based upon multi hop communication architecture specifically designed for homogeneous WSN. Clustering based protocols, AP (Asymmetric pre-distribution) scheme and CKP (Clustering based Key management Protocol) are proposed for heterogeneous WSN. Simulations are done in MATLAB. Results of simulation declare that CKP outperforms other two schemes in terms of transmission distance, memory burden, energy dissipation and resilience.

III. PROBLEM FORMULATION

The key mechanism alone can not provide adequate to all necessary communication that is required for operation in the network WSN protection. Furthermore, the performance in terms of consumption of resources and security must be balanced to make use of different types of keys.

The degree of key exchange in the security mechanism has to be taken into consideration. For example, if the only key pairs are used for every two nodes in WSNs for secure communication, the node captured by an attacker not reveal any safety information other normal nodes, which is ideal to avoid threatening entire network. However, it requires significant resources bandwidth communication and energy, which is quite inefficient. On the contrary, if only a key across the network is used for authentication and encryption, no communication between nodes for the establishment of additional keys are required, and storage costs and power consumption can also be minimized . However, security will be very poor. Once any node in the system is captured by an attacker, the entire network undergoes a huge risk.

A. WORK DESCRIPTION:

- Examine the current state of WSNs and the possible future that they may provide. Any applications that a WSN may be deployed in will be identified as well as their generic requirements. Once these requirements have been determined they should be investigated as to what effect they will have on the protocol and the WSN.
- Investigate the multitude of security techniques that are available.
- Identify advantages and disadvantages of the various security architectures being employed.
- Examine currently available simulators for WSNs.
- Investigate the credibility of research to date.

IV. PROPOSED SCHEME

The design of the basic schemes used were motivated by the observation that single keying mechanism is not suitable for meeting all the security requirements of different types of exchanged messages. The advantage of this scheme is that the captured node does not threat the safety of the other nodes in case the master key K is absolutely safe in time interval Tmin.

During the time interval Tmin, all the nodes of the WSN will hold the general master key K and we note that this scheme cannot provide confidentiality when a node is compromised in Tmin. Because, by using the stolen information like the master key K, an attacker can easily derive the master keys of all the rest normal nodes that are deployed in the same time interval as well as negotiating new pairwise key with normal nodes in any region, which means once a node is compromised in time interval Tmin, the security of the entire network is extremely dangerous.

By enhancing the existing techniques we can avoid the different shortcoming with modified steps. The steps involved and detail of the proposed technique can be presented as:

i. Proposed modified technique is based on Diffe-Hellman algorithm.
ii. Prior to deployment of the network, each node prestores a set of prime number p and its primitive root a instead of the initial key k or any key derived from the master key.
iii. Individual key for a node A can be derived as : $K_A = f(K_1, A)$
iv. This key is generated from the function which is known as the individual key and on generation of the individual key the key prior present as a derived key from the master key for the network is deleted.
v. This avoid any information to attacker in case , the stored information is accessed.
vi. Key evolution function, taking P and Q as two nodes
$X_P = h(P|K_P) \bmod p$
$X_Q = h(Q|K_Q) \bmod p$
The public message can be calculated as:
$Y_P = a^{X_P} \bmod p$
$Y_Q = a^{X_Q} \bmod p$
vii. The pairwise key can be generated as
$K_{PQ} = (Y_P)^{X_B} \bmod p$
viii. These pairwise keys are used for the communication between the nodes.

V. RESULTS

On the basis of simulation we have collected, we have many results; these results are in the form of graphs. The graphs are ploted for Number of dead Nodes, Alive node percentage, Packets to Base Station and Number of Cluster Heads. These graphs values are plotted with respect to number of Rounds.

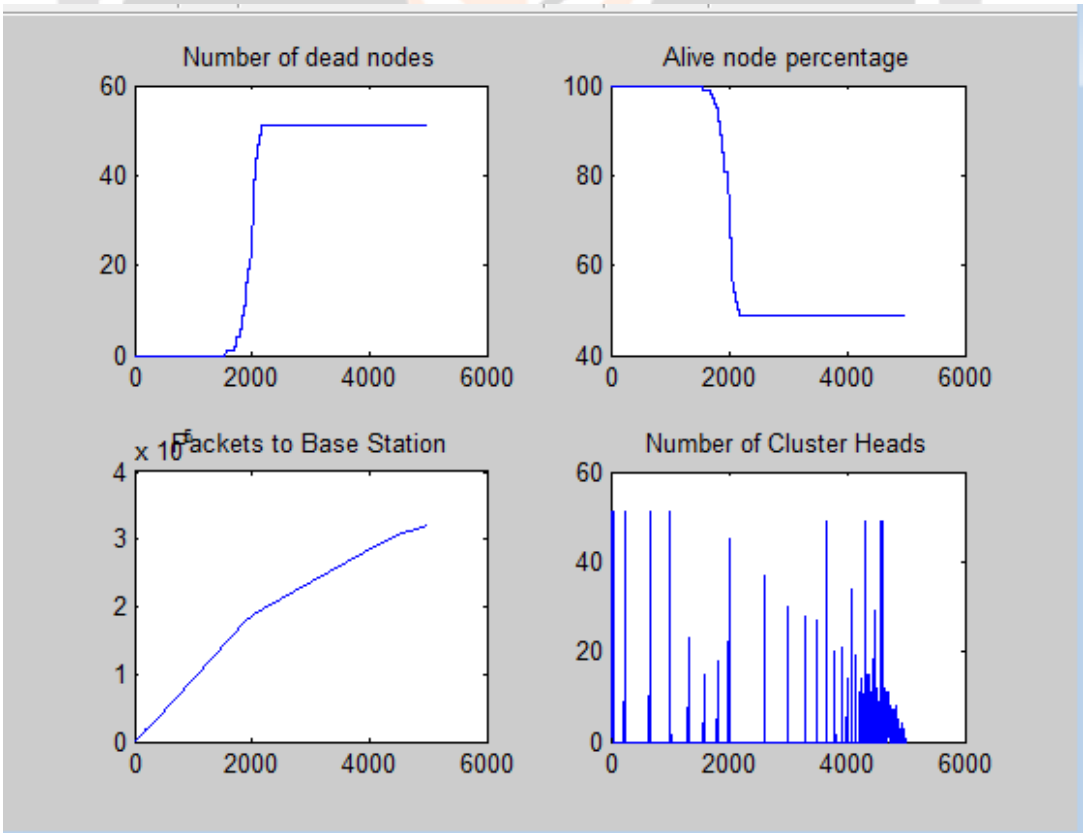

Figure 1: Plot of different parameters

VI. CONCLUSION

The security mechanism available for the key exchange lacks in the security when some attacker gets the access to the stored information in the nodes. With this information the attacker can get the information of the master key and with the help of the master key , it can get the information of the master key which is further helpful to derive the other keys in the network thus penetrating in the whole network. The proposed security technique make use of the master key and key derived from this but after this it generates the individual key with the help of the Diffie-Hellman algorithm. This algorithm is able to generate the individual key for each node and encrypt the derived key from the master key in such a way that it can be further extended to individual key. After the generation of individual key the derived key from the master key which can be used to get the information about the master key is deleted and the new individual key generated as a result of encryption in retained and this is further used for the pairwise key generation and authentication of nodes for the communication. The communication done is much secure because even the information is stolen from any of the node present in the network the master key is not obtained. The security level is increased by the modified approach for the secure communication and without increasing the storage space requirements.

REFRENCES

[1] M. Palit and R.C. Biradar "A Survey on Routing Protocols in WSN", Networks (ICON), 18th IEEE International Conference on Dec. 2012,

[2]Rathna and Sivasubramanian, "Improving Energy Efficiency in Wireless Sensor Networks through Scheduling and Routing", Research Scholar, Sathyabama University, TamilNadu, India, International Journal of Advanced Smart Sensor Network Systems, vol: 2, pp: 21-27, January 2012.

[3]Shio Kumar Singh, M P Singh, D K Singh, "A Survey of Energy-Efficient Hierarchical Cluster-Based Routing in Wireless Sensor Networks", International Journal. of Advanced Networking and Applications, vol: 02, pp: 570-580, 2010.

[4] Honey Soni, Priyanka Tripathi and Robin Singh Bhadoria, "An Investigation on Energy Efficient Routing Protocol for Wireless Sensor Network", Computational Intelligence and Communicational network, vol: 7, pp: 141 - 145, Sept. 2013.

[5] Deepa H, Aayan Kumar Daas ," A Study on Routing Protocols in Wireless Sensor Network" , published in: International journal of computer applications, vol: 72,pp-35-39 , 2013.

[6]Seyedeh Zahra Yazdanpanah, Yousef Abbasnejad Varzi, Ali Haronabadi, "An Improved energy Consumption Method For WSN", Fuzzy Statement and Knowledge Discovery, vol:-4, pp:-1123-1132, 2014.

[7] Li Ya, Wang Pengjun, Luo Rong, Yang Huazhong, Liu Wei," Reliable Energy-Aware Routing Protocol for Heterogeneous WSN Based on Beaconing", Advance Communication Technology(ICACT), vol:-8, pp:109-112 , Feb 2014.

[8] Al-Karaki, J.N, "Routing Techniques in WSN: A Survey", Wireless Communications, IEEE, vol: 11, pp: 6-28, Dec. 2004.

[9] Jia Xu,Ning Jin, Xizhong Lou,Ting Peng,Qian Zhou,Yanmin Chen, "Improvement of Leach Protocol for WSN",Fuzzy System and Knowledge Discovery(FSKD), , vol:-11, pp:-2174-2177 May. 2012.

[10] Yamunadevi, S.P,"Efficient Comparison of Multipath Routing Protocols in WSN", Computing Electronics and Electrical Technologies (ICCEET), vol: 2, pp: - 807-811, mar. 2012.

[11] Jianguo SHAN, Lei DONG, "Research on Improved Leach Protocol of WSN", IEEE, pp:-75-77, 2013.

[12] Chunyao Fu, Zhifang JIANG, Wei WET, "An Energy balanced Algorithm of Leach Protocol in WSN", International Journal of Computer Science, vol:-10, pp:-354-359, 2013.

[13] Yun Li, Nan Yu, Weiyi Zhang, Weiliang Zhao, "Enhancing the Performance of Leach Protocol for WSN", IEEE INFOCOM, pp:-223-228, 2011.

[14] Laveena Mahajan "Improving the Stable Period of WSN using Dynamic Stable Leach Election Protocol" Issues and Challenges in Intelligent Computing Techniques (ICICT), vol-11, pp: 393-400, 2014.

[15] Huu Nghia Le, Vyacheslav Zalyubovskiy, Hyunseung Choo "Delay-minimized Energy-efficient Data Aggregation in Wireless Sensor Networks", International Conference on Cyber Enabled Distributed Computing and Knowledge Discover (IEEE), vol-1, pp: 401-407, Oct. 2012.

[16] Linlin Wang, JieLiu, Wei Wang "An Improvement and Simulation of LEACH Protocol for Wireless Sensor Network", First International Conference on Pervasive Computing, Signal Processing and Applications (IEEE), pp: 444-447, Sept. 2010.

[17] Ma Chaw Mon Thein, ThandarThein "An Energy Efficient Cluster-Head Selection for Wireless Sensor Networks", International Conference on Intelligent Systems, Modeling and Simulation (IEEE), vol:-8, pp.287-291, Jan. 2010.
[18] Meenakshi Sharma and Anil Kumar Shaw "Transmission Time and Throughput analysis of EEE LEACH, LEACH and Direct Transmission Protocol: A Simulation Based Approach", Advanced Computing: An International Journal (ACIJ), vol: 3, pp: 5-9, September 2012.
[19] M M Islaml, M A Matin2, T K Mondol l "Extended Stable Election Protocol (SEP) for Threelevel Hierarchical Clustered Heterogeneous WSN", (IEEE), vol: 5, pp. l -4, June 2012.
[20] Reetika Munjal, Bhavneesh Malik "Approach for Improvement in LEACH Protocol for Wireless Sensor Network", Second International Conference on Advanced Computing & Communication Technologies (IEEE), pp.517-521, Jan. 2012.