Novel method for secure key management in Wireless environment

Mr.Abhijit S.Bodhe

PhD Scholor, Department of Computer Science Engineering, Visvesvaraya Technological University, Belgaum, Karnataka

Asst. Prof. at Sanjivani College of Engineering, Kopargoan, Maharashtra, India. bodhe.abhijit@gmail.com, ORCID:- https://orcid.org/0000-0001-7073-4876

Dr. Prahantha G.R.

Associate professor, Dept. Of computer science and engg. Jain institute of technlogy, Davanagere, KA, India. prashanthagr.sjce@gmail.com

***Abstract*— The wireless sensor network (WSN) has important applications like remotely monitoring environment and tracking of targets, basically in recent few years using multiple sensors which are intelligent, faster smaller and cheaper in cost. WSNs uses wireless communication with multi-hop routing for transfer of digital data, introduces more routing attacks on network. The security attributes are the mechanisms which allow the routing protocols to defend against the possible threats in the whole network. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs.**

Proposed paper is to show that, when the designed algorithm/s developed in the Network Simulator (NS-2) tool environment is run, the automatic security of the data is done even when the attackers play an important role in hacking the data by corrupting it. , we are going to propose 3 novel methodologies for secure key management framework in dynamic mobile wireless sensor networks.

Keywords—WSN, Authentication, Sensor, Node, Network, Key, Message Authentication Code Protocol, Security, Routing, Management, , Cryptography, Source, Energy, Router, Attacker)

I. INTRODUCTION

In this introductory section, a brief review of the concepts relating to the wireless sensor mobile networks, its types, structure of the WSN. A "*Wireless Sensor Network*" is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

The 1st work would be related to the development of an energy-efficient & reliable routing protocol for m-WSNs using hierarchical and cluster based E2R2 approach, The 2nd work would be related to the development of a forward authentication key management scheme for heterogeneous sensor networks with key encryption, key revocation. The 3rd work would be related to the development of a secured & energy efficient clone detection protocols in h-WSNs with improvement in key generation

WSN refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking, particularly in recent years with the help of sensors that are smaller, cheaper, and intelligent.

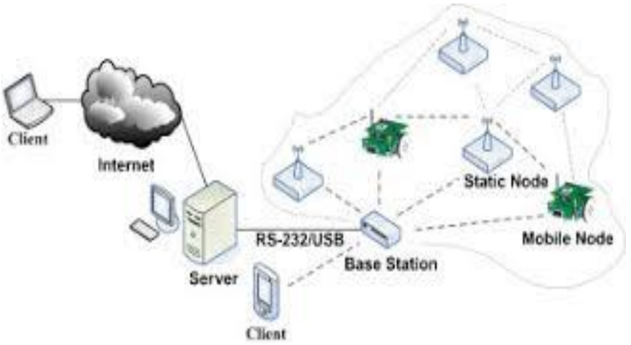

Fig. 1.1 : General structure of a static WSN

DOI : 10.35291/2454-9150.2021.0341

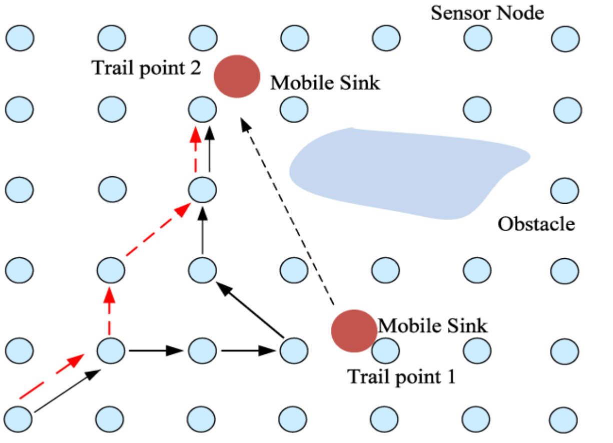

Fig. 1.2 : General structure of a *m*-WSN

The static schemes assume that once administrative keys are pre-deployed in the nodes, they will not be changed. Administrative keys are generated prior to deployment, assigned to nodes either randomly or based on some deployment information, and then distributed to nodes. For communication key management, most static schemes use the overlapping of administrative keys to determine the eligibility of neighbouring nodes to generate a direct pair-wise communication key. Communication keys are assigned to links rather than nodes. In order to establish and distribute a communication key between 2 non-neighbouring nodes and/or a group of nodes, that key is propagated one link at a time using previously established direct communication keys [24], this is what is called as static KMS.

In this section, some overview about the dynamic key management issues has been presented in a nutshell. Key management schemes in sensor networks can be classified broadly into dynamic or static solutions based on whether rekeying (update) of administrative keys is enabled post network deployment. The objective of key management is to dynamically establish and maintain secure channels among communicating nodes. Numerous key Management schemes have been proposed for sensor networks. Most existing schemes build on the seminal random key pre-distribution scheme introduced by Eschenauer and Gligor [14]. Dynamic key management schemes may change administrative keys periodically, on demand or on detection of the node capture. The major advantage of the dynamic keying is enhanced network survivability, since any captured key/s is replaced in a timely manner in a process known as re-keying. Another advantage of dynamic keying is providing better support for network expansion; upon adding new nodes, unlike static keying, which uses a fixed pool of keys, the probability of network capture increase is prevented [24].

Key pre-distribution is one of the solutions to the problem of the key establishment in WSNs, where a finite set of keys is assigned to each sensor node before deployment of the network. Key pre-distribution schemes can be classified into 3 categories, viz., random, deterministic, and hybrid [13]. These schemes do not ensure direct communication between every pair of nodes through a common key. If the 2 nodes cannot communicate directly, a path need to be established between them. Establishing a path key increases energy consumption & decreases the speed of communications.

One of the important paper concepts that may be thought of is providing of the security by the dynamic key management for different category of applications such as secure clustering secure routing (SCSR) etc, which is thought of in our paper after seeing the previous works. These schemes may provide better packet delivery ratio and security by considering the efficient usage of energy.

II. Literature

Xing Zhang, Jingsha He and Qian Wei proposed a distributed deterministic key management scheme for WSNs. It concentrates on pairwise key establishment as well as maintenance of the keys that includes local clusters also. EDDK supports node mobility and node addition during the lifetime of the network. It uses elliptic curve digital signature algorithm while establishing the keys for new nodes and mobile nodes. This protocol consumes more storage in maintaining neighbour table if the network size increases. Since the neighbour table is limited to a threshold, sometimes a new trusted node may not be able to join the network, which was a major drawback in their paper [8].

Ramzi Bellazreg and Noureddine Boudriga have proposed a group key management protocol suitable for HWSNs. This protocol uses the secure tunnelling approach that ensures multiple nodes can communicate among them using the same tunnel. They have introduced the cluster security association concept that establishes many-to-many tunnels to represent the attributes related to the security between many sensor nodes in the network. The clusters are formed based on the locations of the similarly detected events by the sensor nodes. To improve the security and protect the network from node compromise attack, the protocol changes the tunnel key periodically in distributed manner without the dependence of the BS. Also, the new sensor nodes are included in the network securely. Results showed that this protocol consumed less memory space and reduced processing and communication overheads. In their work, two mobility models of the targets were only considered & work was not carried out on multiple targets, which was a major drawback [9].

Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo worked on the security issues using block chain futures in the IOT in WSNs. The authors surveyed articles presenting IoT security solutions for more than a decade & presented in their paper relating to the same. They made some number of observations, including the

DOI : 10.35291/2454-9150.2021.0341

lack of publicly available IoT datasets that can be used by the paper and practitioner communities. They showed that there is a need to develop a standard for sharing IoT datasets among the paper and practitioner communities and other relevant stakeholders & hence posited the potential for block chain technology in facilitating secure sharing of IoT datasets. Optimization of bloc chains and block chain-based platforms were not dealt with, which was a major drawback [10].

Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Abdul Sattar and Vijay Varadharajan worked on dynamic authentication schemes for hierarchical WSNs. The authors developed a security scheme for monitoring apps. They proposed a decentralized authentication and key management network for hierarchical ad hoc sensor networks & the scheme was light weight and energy aware, thus reducing the communication overhead. To resist against malicious attacks, secure communication between severely resource-constrained sensor nodes was made necessary while maintaining scalability and flexibility to topology changes. One drawback of their scheme was that if the sensor nodes in one cluster change frequently, the group key will have to be changed as a result of which the transmission time increases [11].

Dynamic key distribution in WSNs with reduced communication overhead was papered upon by Ramu Kuchipudi, Dr. Ahmed Abdul Moiz Qyser & Dr. Balaram in their paper presented in [12]. In order to protect the sensitive data in WSNs, secret keys were used to encrypt the exchanged messages between communicating nodes, thus projecting an effective method of key management in their paper. Symmetric or asymmetric key cryptography or trusted-server schemes were used to solve this security problem. They proposed Mobile Agent (MA) Based Key Distribution (MAKD) to reduce the communication overloads in b/w the nodes & the mobile agents were used for dissemination of public keys and update of shared keys. One drawback in their work they made use of only cluster heads & considered only very few nodes for the simulation [12].

In majority of the work done by the various authors presented in the previous paragraphs [1] - [30], there were certain drawbacks / disadvantages / lacunas such as consideration of only

- use of conventional methods,
- high compilation time,
- computationally very expensive,
- full-fledged automation of security deployment not done,
- less work done on increasing the accuracy & performance,
- real time implementation (h/w), very few people done, etc.,
- pool size & number of sensors was medium,
- overheads of computation & transmission problems were more,
- some developed protocol was not able to deliver good results,
- not energy efficient and scalable,

III. Objectives of Paper

First, confirm We actually, aimed to develop sophisticated security network algorithms in the event of data attackers from the hackers in the field of wireless sensor and mobile dynamical networks, which is our main desired objective and also to develop some automated GUIs for the same. This objective is going to be achieved using the short range / long range objective steps in a course of 4+ years & mentioned in the subsequent pages. Our objectives is being broken down into smaller objectives, which are mentioned as under……

- The focus of future paper work objective is towards the security by designing dynamic key management. The design of a simple key management approach for static homogeneous wireless sensor networks along with re-keying support to refresh the secret keys whenever required.

- The focus of this objective is mobility and security of the network support by development of dynamic key management. To design a secure key management protocol for mobile wireless sensor network that manages the node mobility for the lifetime of the network.

- To understand the work done by various authors till date in the relevant field & to define the paper problem by considering their future works & some of their drawbacks.

- Collecting the data's of the structure of the WSNs with the source nodes, sink nodes & the attacker nodes.

- Developing .ns2 (tcl) code or AWK for the process in the previous mentioned steps, observing the results, tabulation of the results obtained and determining the authenticity of the work implemented.

- Comparison of the developed methodologies for the best performance.

- Comparison of the proposed works with the work done by other authors, thus validating the supremacy of the proposed paper work done..

IV. PROBLEM STATEMENT

Before A recent survey by world security organisation states that data security is being a lot of importance in the modern days as hackers are trying to steal the data by hacking the information, especially the banking info, students info, defense info, aadhar info, etc…., which is a

DOI : 10.35291/2454-9150.2021.0341

serious threat to the nation's security. In this context, we thought that to do some service to the nation's security by developing some protocols by increasing the security using providing key encryption schemes & by other means

The main motivation being some of the current security initiatives w.r.t. the defense issues taken up by the state & central government in the wake of terrorist activities in the country, this was the root cause for our motivation. Hence in continuation, with zeal of this work & to carry out further in this regard to do something to the society in the case of security issues, we are proposing some new methodologies for introducing the security keying issues in WSN

V. Proposed Paper Methodology

The proposed methodology for development of enhanced secure key management framework in dynamic mobile wireless sensor networks is being presented along with a block-diagram (may change in the near future).

1.Development of an energy-efficient & reliable routing protocol for m-WSNs using hierarchical and cluster based E2R2 approach

2.Development of a forward authentication key management scheme for heterogeneous sensor networks with key encryption, key revocation, addition of a new node & and the generation of a new key-chain w.r.t. base station and cluster heads

3.Development of a secured & energy efficient clone detection protocols in h-WSNs with improvement in key generation, encryption & decryption using RSA/SHA or any simple security algorithm

Due to the dynamic changes in the network, the security has to be given more importance in order to protect the data as well as to maximize the lifetime of the network. While providing the security for the network, the key management plays a major role in it. Using a single network wide key gives up the entire network if the single key has been compromised. By using pairwise keys, it improves the security as well as the lifetime of the network but lacks in scalability due to the memory constraint. Thus, changing the key dynamically provides more security and also improves the lifetime of the network. The parameters that are used for dynamic key generation should be chosen carefully in such a way that the intruders should not predict them. Since the keys are dynamically changed, it increases the communication overhead in order to share it with the neighboring nodes or the destination. This overhead can be reduced by the design of key management techniques or by modifying of the protocol. It has to be noted in this context that the key deployment is similar to the OTP generation in the mobiles for secure transactions. Since many applications require the support of mobility, the dynamic & efficient clustering algorithm has to be designed w/o compromising the security of the n/w. The network architecture also plays an important role in providing security and doing complex tasks such as key management, secure clustering, secure routing etc. Deploying more number of heterogeneous nodes improves the performance of the network but it is not cost effective. So the heterogeneous nodes have to be deployed optimistically in the field.

V. Discussion Remark

The final result or the final outcome or the end-result of the paper work is aimed to develop some efficient security keying management protocols for the secure data transmission from the source node to the sink nodes via a number of cluster heads even in the presence of attacker nodes trying to corrupt & hack the data transmission process, taking some of the network parameters such as time, energy, communication, network speed, memory performance, data transfer rate, security keying, decryption, encryption, etc….

The main outcome being, when the designed algorithm/s are run with the input given, the automatic data transmission takes place with good computational time in comparison with the work done by the other papers till date taking into consideration many of the drawbacks of the fellow papers, thus enhancing and improving the performance of the existing algorithms.

The parameters such as network resilience, speed of transmission, communication overhead, computation overhead and energy consumption are also analyzed while designing the key management part in the security solutions, which are some of the possible outcomes. A security for mobile Heterogeneous WSNs (mH-WSNs), the parameters such as packet delivery ratio, network availability, data availability, energy consumption could be analyzed which are other possible outcomes, which are also tackled with in the proposed paper work.

References

[1] G. Eason, B. Noble [1] Majid I. Khan, Wilfried N. Gansterer, Guenter Haring, "Static vs. mobile sink : The influence of basic parameters on energy efficiency in wireless sensor networks", Comp. Communications, Vol. 36, No. 9, pp. 965–978, May 2013.

[2] https://en.wikipedia.org/wiki/Mobile_wireless_sensor_network

[3] https://en.wikipedia.org/wiki/Wireless_sensor_network

[4] http://www.ni.com/white-paper/7142/en/

[5] Xiaobing He, Michael Niedermeier, Hermannde Meer, "Dynamic key management in wireless sensor

DOI : 10.35291/2454-9150.2021.0341

networks: A survey", Jour. of Network & Comp. Applications, Vol. 36, Issue 2, pp. 611-622, Mar. 2013.

[6] Qiu Ying, Zhou, Jianying, Baek, Joonsang, and Lopez, Javier, "Authentication and key establishment in dynamic wireless sensor networks", Jour. of Sensors, ISSN 1424-8220, Vol. 10, No. 4, pp. 3718-3731, 2010.

[7] Seung-Hyun Seo, Jongho Won, Salmin Sultana and Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE Trans. on Info. Forensics & Security, Vol. 10, No. 2, pp. 371 – 383, Feb. 2015.

[8] Xing Zhang, Jingsha He and QianWei, "EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks", Hindawi Publishing Corporation EURASIP Jour. on Wireless Communications & Networking, Vol. 2011, pp. 1-11, Article ID 765143, 2011.

[9] Ramzi Bellazreg and Noureddine Boudriga, "DynTunKey : a dynamic distributed group key tunnelling management protocol for heterogeneous wireless sensor networks", EURASIP Jour. on Wireless Comm. & Networking, paper id 2014:9, pp. 1-19, 2014.

[10] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo, "A block chain future for internet of things security: a position paper", Elsevier's Dig. Comm. & Networks, Vol. 4, pp. 149–160, 2018.

[11] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Abdul Sattar and Vijay Varadharajan, "A Dynamic Authentication Scheme for Hierarchical Wireless Sensor Networks", Mobile & Ubiquitous Systems : Computing, Networking & Services, 7th Int. ICST Conf., MobiQuitous-2010, Tokyo, Japan, Dec. 2–4, 2013.

[12] Ramu Kuchipudi, Dr. Ahmed Abdul Moiz Qyser, Dr. V.V.S.S.S Balaram, "A Dynamic Key Distribution in Wireless Sensor Networks with reduced communication overhead", Int. Conf. on Electr., Electron. & Optimization Techniques (ICEEOT) – 2016, pp. 3651-3654, Chennai, Tamil Nadu, India, 3-5 Mar. 2016.

[13] Seyed Hossein Erfani, Hamid H.S. Javadi and Amir Masoud Rahmani "A dynamic key management scheme for dynamic wireless sensor networks", Security & Comm. Networks, Vol. 8, No. 6, pp. 1040–1049, Jun. 2014, Apr. 2015.

[14] Eschenauer L., Gligor V.D., "A key-management scheme for distributed sensor networks", Proc. of the 9th ACM Conf. on Comp. & Comm., Sec., ACM, Washington, DC, USA, pp. 41–47, 2002.

[15] Çamtepe S.A., Yener B., "Combinatorial design of key distribution mechanisms for wireless sensor networks", IEEE / ACM Trans. on Networking, Vol. 15, No. 2, pp. 346–358, 2007.

[16] Lee J., Stinson D.R., "On the construction of practical key pr-distribution schemes for distributed sensor networks using combinatorial designs", ACM Trans. on Info. & Syst. Sec. (TISSEC), Vol. 11, No. 2, pp. 1–35, 2008.

[17] Ruj S., Roy B., "Key pre-distribution using partially balanced designs in wireless sensor networks", Jour. of Parallel & Distributed Processing & Apps., Springer - Berlin Heidelberg, pp. 431–445, 2007.

[18] Dong J.W., Pei D.Y., Wang X.L., "A class of key pre-distribution schemes based on orthogonal arrays", Jour. of Comp. Sci. & Tech, Vol. 23, No. 5, pp. 825–831, 2008.

[19] Ramu Kuchipudi, K. Vaishnavi Prapujitha, Y.G Shantha Reddy, "A Hamming Distance Based Dynamic Key Distribution Scheme for Wireless Sensor Networks", Int. Jour. of Engg. & Comp. Sci., ISSN : 2319-7242, Vol. 2, No. 11, pp. 3197-3201, 2013.

[20] Ganesh R. Pathak and Suhas H. Patil, "A Hybrid Novel Perspective of Secure Routing in Wireless Sensor Networks", Indian Jour. of Sci. & Tech., Vol. 9, No. 10, pp. 1-8, Mar. 2016.

[21] Paulo F. Oliveira, João Barros, Member, "A Network Coding Approach to Secret Key Distribution", IEEE Trans. on Info. Forensics & Sec., Vol. 3, No. 3, pp. 414-423, Sept. 2008.

DOI : 10.35291/2454-9150.2021.0341