Proceedings of
National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015)
held at BRCMCET , Bahal on 4th April 2015

A theoretical analysis of Self-adaptive decentralized selective jamming (SAD-SJ) against DoS and DDoSattacks in WSNs

[1]Harsimran Kaur, [2]AmanPreet Singh , [3]Dr. Rohit Bajaj
[1,2]Research Scholars, [3]Associate Professor
,Department of Computer Science & Engineering, CEC College, Landran , India,
[1]matternature21@gmail.com , [2]amansingh6940@gmail.com , [3]cecm.cse.rohitbajaj@gmail.com

Abstract—This paper studies the effectiveness of Self-adaptive decentralized solution against selective jamming (SAD-SJ attacks in WSNs. The SAD-SJ has been thoroughly studied for its effectiveness against the DoS and DDoS attack using the selective methods on the wireless sensor networks. The theoretical studies has been shown that SAD-SJ is not enough efficient against the target attacks and requires some major improvements in its design to become efficient enough to protect against such attacks.

Keywords: SAD-SJ, DoS, DDoS, WSN security, selective jamming, self -adaptive decentralized solution

I. INTRODUCTION

The evolution of wireless sensor networks has become one of the predominant technology of research and development .The elementary objective of WSN is to accumulate data from the environmental world. The involvement of wireless communication technology further induces numerous types of security hazards .The security of wireless sensor network is intensely crucial. A Wireless Sensor Network (WSN) is a compilation of sensor nodes, which forms up a network utilizing radio communication in an independent and dispersed manner. These sensor nodes are scattered over a distinct terrestrial space and are capable to assemble and broadcast information about the habitat, in order to provide exquisite observations of a facts.

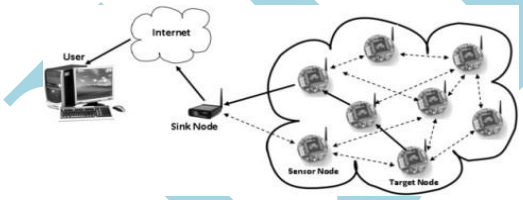

Fig1 : WSN Architecture

The sensory nodes are typically supplied with one or more sensors that are employed to capture acts from the environment, an analog-digital converter, aradio transceiver, a central processing unit with definite computing capacity, a limited chunk of memory and a battery power supply. Sensor devices cooperate with each other in order to execute fundamental activities such as sensing data, communication and processing of data.

The leading applications of WSNs consists of: observing environment, health care, mood-based services, positioning and animal tracking, entertainment, logistics, transportation, home-based and office, industrial and military applications. Non-intrusive and non-disruptive environmental monitoring benefits botanist to examine perceptive the habitats of wildlife for instance the micro-climates on Great Duck Island, Maine. The Health care applications of WSN allow human beings with certain therapeutic conditions to obtain consistent auditing through sensors. Militant functions involve surveillance, tracking of targets, counter-sniper systems and controlling battlefield, in which he is propagated to soldiers and vehicles involved in encounter.

The technological progress in wireless communication and microelectronics have arised in increasing importance in the field of wireless sensor networks. A sensor network comprises of deployment of cluster of sensors nodes for distributed monitoring of actual time events. The sensor networks have restricted power supply, as the sensor nodes are powered with batteries which is one of the critical issue in WSN. There has been an expanding use of sensor networks for life critical operations such as monitoring patients in hospitals and military applications. These applications make it substantial to have a great infrastructure of security for sensor networks.

The disposition of these networks in militant applications and the limited power of battery and memory, makes the architecture of a security protocol dispute.

The security of Wireless Sensor Networks(WSN) can be compromised in many ways. A distant end user that access base station information can be interrupted from doing so in a variety of ways. The transmission between the base station and sensor nodes can be halted. This can be achieved by analog compressing of signals or by computerized jamming in the form of DoS(Denial of Service) attacks that flow in the network,sink or both.

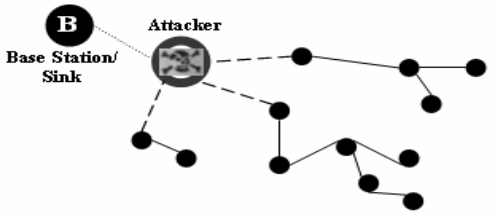

Fig2: Attack in WSN

Another way of violating security is to damage the base station itself. This can be attained by controlling the quantity and direction of packet transit toward the base station so that the location is eventually disclosed. Eavesdropping can be used to record and understand the position of the base station for demolition. There are several other techniques to breach the WSN security.

Several attacks begin because of the loss of security in the inter communications of sensor nodes. For instance, a hacker can easily build a connection with the insecure wireless sensor nodes to affect or jam the whole sensor network. These types of attacks can be reduced or blocked by applying key exchange mechanisms which deal with the secure cryptographic keys between the sensor nodes to protect the security of communications.

During the extent of time when the WSN nodes are in occupied condition, they need secure cryptographic keys for safe procreation of the hypersensitive information. Efficient key management and distribution scheme play an essential part for the protection of data in WSNs. The existent cryptographic key management and distribution technique usually spend great quantity of energy and put larger calculation costs on Wireless Sensor Nodes.The cryptographic keys are used on distinct communication layers of WSN communications i.e. neighboring nodes, cluster heads and base stations. An efficient corporate key management and distribution procedure is mandatory to manage the security of the wireless sensor networks.

II. LITERATURE REVIEW

Marco Tiloca, et. Al. Have projected wireless sensor networksarepresentlyemployedin severalapplication situation s, as well asindustrial applications and manufacturing plant automation. In such situations, Time Division Multiple Access (TDMA) is usually used for digital communication among sensor nodes. However, TDMA-based wsn's are notably at risk ofspot jamming attack, a particular variety of Denial of Service attack geared toward severely thwarting network responsibility. During this paper, we have briefly studied to present SAD-SJ, a self-adaptive in nature anddecentralized MAC-layer resolution against spot-jamming in TDMA-based wns's. SAD-SJ doesn't want a central entity, needs sensor nodes to believe solely on native info and permits them to affix and leave the network without preventive alternative nodes activity. We have a tendency to show that SAD-SJ introduces a restricted overhead, in terms of computation, communication and energy consumption.

Zongwei zhou et. al. have projected a new key management system named KISS within which the matter of fine-grained key usage management and secure system administration are solved. KISS primarily aims at reducing cost by counting on hardware and minimizes the system TCB by creating the utilization ofthin-hypervisor-based style and light-weight administrator devices. KISS provides user-verifiable trustworthy methods and straight forward dedicated external devices for secure system administration.**N.**

Suganthietet. al. have planned an algorithmic rule to support the institution of 3 kinds of keys for every sensing element node, a private key shared with the base station, a pair wise key shared with neighbor sensing element node and a bunch key that's shared by all the nodes within the network.The algorithmic rules used for establishing and changing these keys are energy economical and minimizes the involvement of the base station. Polynomial function has been used for key generation purposes.

Ivan Damgardet. al.have projected a secure key management technique for cloud environments. Authors have studied the amount of security on the idea what they will and what they can't getwithin the security models. And once finding out that all, authors have planned a light-weight protocols achieving supreme security, and report on their sensible performance. They have thought-about totally autonomous servers that switch between online and offline periods while not communicating with anyone from outside the cloud, abd semi-autonomous servers that require a restricted reasonably help from outside the cloud when doing the transaction.

RamaswamyChandramouliet. al.have worked on cryptological key management issues and challenges in cloud services. An analysis of the common state of observation of cryptological operations that supply those security capabilities reveals that the management of cryptological keys takes on an extra-quality in cloud environments compared to enterprise IT environments due to:
(a) distinction of possession (between cloud customers and cloud Providers), and
(b) management of infrastructures for every Key Management System (KMS) and guarded resources square measure settled. This document identifies the cryptological key management challenges at various intervals of the context of subject solutions that are usually deployed to perform those cryptological operations.

III. STUDY OF SAD-SJ

The existing security mechanism is called "Self adaptive decentralized solution against selective jamming attack in WSN". The selective jamming attack is a form of denial of service attack, which is used to cause the resources unavailable for particular purpose. Self-adaptive in the title means that each node is individually capable of tacking the selective jamming attack on their own. The proposed model is applicable for the wireless sensor network working on TDMA (time division multiple access) and effective against denial of service attack (DoS attacks only). The proposed scheme is aimed to work at MAC layer. Also the proposed scheme is aimed to solve the problem of energy consumption. The new scheme in the paper is created to put the least effect on the energy consumption and helps the WSN to last longer when the security scheme is implemented.

SHORTCOMINGS OF THE SAD-SJ

1. The self adaptive decentralized solution against selective jamming attack is effective against the denial of service (DoS) attacks only.Most of the attacks launched on the WSNs are distributed denial of service (DDoS) attacks, which is not protected using this scheme.

2.The security scheme in base paper is very complex.The packet exchange between the nodes according to the scheme adds a heavier overhead on the WSNs.

3.The security scheme in base paper is based on a formula to find the integral code for authentication purposes.The

permutation method is used to embed and verify the secure code, which is prone to hacking because it is based on a mathematical formula.

IV.CONCLUSION

In the paper, we have evaluated the SAD-SJ method for its performance in the case of WSNs. The SAD-SJ techniques is used to prevent the DoS and DDoS attacks. The existing scheme has been thoroughly analyzed for its performance in the case of both of the attacks. The existing is found not efficient enough to prevent against such attacks. The SAD-SJ Mechanisms must be improved in order to make it capable of effectively protecting against selective jamming (DoS or DDoS) attacks. The SAD-SJ can be improved by adding stronger and efficient key management methods.

REFERENCES

[1] Marco Tiloca, Domenico De Guglielmo, GianlucaDini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE, 2013.

[2] Kodali, Ravi Kishore. "Key management technique for WSNs." In Region 10 Symposium, 2014 IEEE, pp. 540-545. IEEE, 2014.

[3] Varadarajan, Prabhakar, and Garth Crosby. "Implementing IPsec in Wireless Sensor Networks." In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on, pp. 1-5. IEEE, 2014.

[4] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate KeyManagement", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.N. Suganthi, V. Sumathy, "Energy Efficient Key Management

[5] Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[6] Ivan Damgård, Thomas P. Jakobsen, JesperBuus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[7] RamaswamyChandramouli, Michaela Iorga, Santosh Chokhani, "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.

[8] Abdallah, Walid, NoureddineBoudriga, Daehee Kim, and Sunshin An. "An efficient and scalable key management mechanism for wireless sensor networks." In Advanced Communication Technology (ICACT), 2014 16th International Conference on, pp. 687-692. IEEE, 2014.

[9] Sahin, Dilan, VehbiCagriGungor, TaskinKocak, and Gurkan Tuna. "Quality-of-service differentiation in single-path and multi-path routing for wireless sensor network-based smart grid applications." Ad Hoc Networks (2014).

[10] Md. MonzurMorshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE, 2013.