ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

COMPRESSED SENSING BASED CLONE IDENTIFICATION FRAMEWORK FOR WIRELESS SENSOR NETWORK

K. Ravi kumar[*1] & D. Kanimozhi[2]

[*1]Asst. Professor, Dept. of Computer Science, Tamil University, Thanjavur-613010.

[2]Research Scholar, Dept. of Computer Science, Tamil University, Thanjavur-613010.

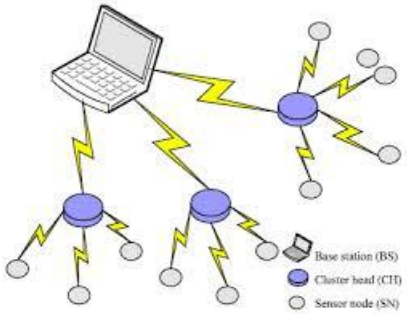
ABSTRACT

One of the mainly vexing problems in wireless sensor network security is the node Clone attack. Aattack, an adversary breaks into a sensor node, reprograms it, with inserts several copies of the node back into the sensor network. Cloning give the adversary and simple way to build an army of malicious nodes that can cripple the sensor network. In for the most part of wireless sensor application security is individual of the prime concern. Generally sensor nodes be not equipped with several tamper resistant hardware and they are deployed in a hostile environment, so the option of occurring attacks should be greater. In node clone attack adversary will capture few nodes since the network, retrieving its credentials with creating large amount of clones by reprogramming the nodes. And these clones can have the ability to subvert the complete network. so the detection of node clone attacks in a wireless sensor network is therefore a fundamental problem. In circulated environment various protocols are available to detect the clone attack. Thus far, various schemes have been proposed to detect replicas; though, mainly of them require expensive hardware like global positioning system (GPS) to obtain the location of a sensor node. In common, sensor nodes be equipped among limited set of resources, to suit for resource constraint sensor application; hence it is not practical to employ additional devices like GPS in them for the detection process.

Keywords: wireless sensor network (WSN), clone attack, intrusion detection, mobility.

1. INTRODUCTION

In Wireless Sensor Networks we detect the clone attacks. The clone nodes are detected by the witness node before the attack occurs. Cloning is normally meant by duplicating the same personality (i.e.) a person who spreads some attacks in network using our name. Our role is to find whether the node is a cloned node or original node before an attack occurs. A wireless sensor network is a collection of nodes organized into a cooperative network. In previous cases, we detect the clone nodes only after the attack occurs.



There is no security process here. If one node sends the data to other, the witness node checks IP address of the node and finds whether it is the original node or a clone node .The witness node can identify the clone nodes only when the clone node and the original node communicates to the same witness node at the same time . A wireless sensor network (WSN) be a remote system comprising of an wide number of physically dispersed sensor nodes. These sensor nodes can be effectively conveyed on vital districts simply at a low cost. Sensor nodes collaborate by one another to screen physical or ecological conditions, used for model, temperature, sound, picture, vibration, weight, progress or contaminations with the assistance of different sorts of sensors. However, while much consideration is constantly paid to the routing strategies and wireless sensor network. the security issues are yet to receive extensive focus. Essentially the utilization of every effective security conspire in wireless sensor classification is encouraged with the span of sensors, the processing power, memory with kind of functions anticipated from the sensors. Sensor networks are not universally traditional computing

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

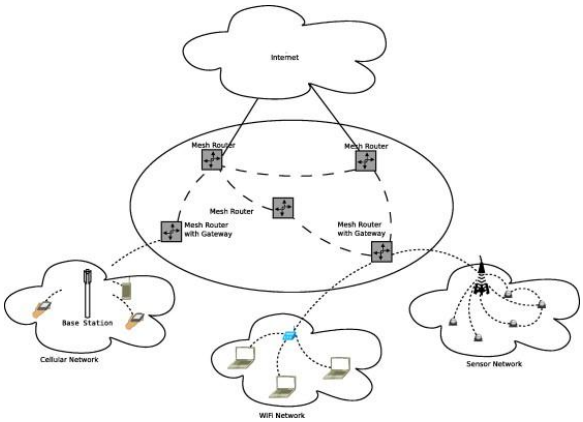
devices; subsequently the existing security models and strategies are lacking to run by them. In sensors, the geographic dissemination of the units allows an attacker to physically have control of nodes and study mystery key material, otherwise to capture messages.

2. RELATED WORKS

The significant advances of hardware manufacturing technology and the development of efficient software algorithms maketechnically and economically feasible a network composed of numerous, small, low-cost sensors with wireless communications, to is, a wireless sensor network. WSNs contain attracted intensive interest from both academia and industry due to their wide application in civil and military scenarios. In hostile scenarios, it is very main to protect WSNs since malicious attacks. Due to different resource limitations and the salient features of a wireless sensor network, the security aim for such networks is significantly challenging. An article, we present a comprehensive survey of WSN security issues that were investigated by researchers in recent years and that shed light on future directions for WSN security. The significant advances of hardware manufacturing technology and efficient software algorithms make a network composed of numerous, small, low-cost sensors, with wireless communication a wireless sensor network (WSN) a promising network infrastructure for many applications such as environmental monitoring, medical care, also home appliance management. This is particularly true for battlefield surveillance and homeland security scenarios because WSNs are easy to deploy for those applications. However, in many hostile with tactical scenarios and important commercial applications, security mechanisms be required to protect WSNs from malicious attacks. Therefore, the security in WSNs becomes an important and a challenging design task[6].

The discrete logarithm method is the foundation of many public key algorithms. However, one type of key, defined as a weak-key, reduces the security of public key cryptosystems based on the discrete logarithm method. The weak-key occurs if the public key is a factor or multiple of the primitive element, in which case the user's private key is not needed but can be obtained based on the character of the public key. An algorithm is presented that can easily test whether there is a weak-key in the cryptosystem. An example is given to show that an attack can be completed for the Elgamal digital signature if a weak-key exists, therefore validating the danger of weak-keys. Methods are given to prevent the generation of these weak-keys[4].

The Nodes Clones feature enables a node to become a clone-node ingroup with other clone-nodes that all share the same content (text, format, icons, etc), appearing because if they were one common node mirrored in multiple places on the map.This feature allows you to take a node-A and make a special-copy of it as a new node-B, so to the contents of node-A become shared (or synchronized) with the contents of the node-B. If the contents of individual of these nodes are manually changed, next the contents of the other node will also be changed - they both share the "same-common-content".as clone-nodes share the "same-common-content" they are visually undistinguishable from each-other in a map - node-A and node-B look the same as they share: similar text, icons, format, etc. So the clone-nodes look like as if they were one common node mirrored in multiple places on the map.



Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first be able to reprogram, with then, preserve replicate them in a large

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

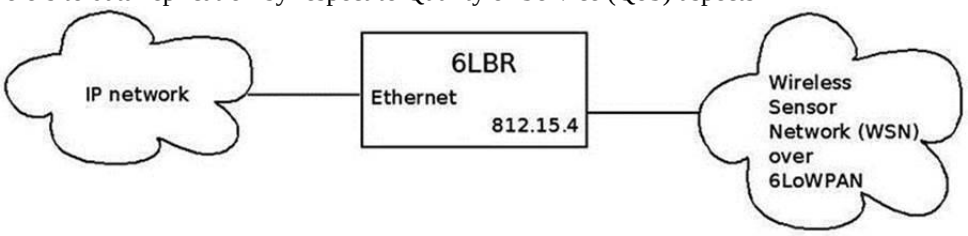
International Journal of Engineering Researches and Management Studies

number of clones, simply taking control above the network. A few distributed solutions to address this fundamental problem have been recently proposed. Though, solutions are not satisfactory. First, they be energy with memory demanding: A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they be vulnerable near the specific adversary models introduced in this paper. The contributions of this work be threefold. First, we analyze the desirable properties of a distributedmechanism for the detection of node replication attacks. Second, we explain that the known solutions for this problem do not completely meet our requirements. Third, we plan a new self-healing, Randomized, Efficient, with Distributed (RED) protocol for the detection of node replication attacks, and we explain that it satisfies the introduced requirements. Finally, extensive simulations confirm that our protocol is highly efficient in communication, memory, with computation; is much more effective than competing solutions in the literature; and is resistant to the new kind of attacks introduced in this paper, as other solutions are not.

3. PROPOSED METHOD

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate to achieve a common goal. WSNs can be deployed in harsh environments to fulfil both military and civil applications . Due to their operating nature, they be often unattended, so prone to different kinds of novel attacks. used for instance, an adversary could eavesdrop all network communications; further, an adversary could capture nodes acquiring all the information stored there in sensors are commonly assumed to be not tamper-proof. Therefore, an adversary can replicate captured sensors and deploy them in the network to launch a variety of malicious activities. This attack is referred to because the clone attack.

Replication in computing involves sharing information so as to ensure consistency between redundant resources, such because software or hardware components, towards improve reliability, fault-tolerance, or accessibility. data replication if the same data is stored on multiple storage devices, computation replication if the similar computing task is executed many times. A computational charge is typically replicated in space, i.e. execute on separate devices, before it could be replicated in time, if it is executed repeatedly on a particular device. Replication in space or in time is regularly linked to scheduling algorithms. The access to a simulated individual is typically uniform by access to a only, non-replicated entity. The replication itself should be transparent to an external user and in a failure scenario, a failover of replicas is unknown as much as possible. The latter refers to data replication by respect to Quality of Service (QoS) aspects



Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), be spatially circulated autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern network be bi-directional, also enable control of sensor activity. The progress of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as developed process monitoring with control, machine health monitoring, with so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. both such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection towards an external antenna, an microcontroller, an electronic circuit for interfacing with the sensors and an energy source, generally a battery or an embedded variety of energy harvesting. A sensor node valour vary in size from that of a shoebox down to the size of a grain of clean, even though functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is also variable, ranging from a few to hundreds of dollars, depending on the complexity of the entity sensor nodes. Size and cost constraint on antenna nodes result in corresponding constraints on resources such as energy, memory, computational speed with communications bandwidth. The topology of the WSNsbe able to vary from a simple star network to an

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

advanced multi-hop wireless mesh network. The propagation technique among the hops of the network can be routing or flooding.

Applications Of Wireless Sensor Network Area monitoring is a common application of WSNs. In area monitoring, the WSN is deploy over a region where some phenomenon is to be monitored. A military example is the exploit of sensors detects enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines

Health care monitoring
The sensor networks for medical applications can be of several types: implanted, wearable, and environment-embedded. The implantable medical devices are those that are inserted inside human body. Wearable devices are used on the body surface of a human or just at close proximity of the user. Environment-embedded systems employ sensors contained in the environment. Possible applications include body position measurement, location of persons, overall monitoring of ill patients in hospitals and at homes.

Environmental/Earth sensing
There are several applications in monitoring environmental parameters, example of which are given below. They contribute to the extra challenges of harsh environments with reduced power supply.

Air pollution monitoring
Wireless sensor networks containdeploy in various cities (Stockholm, London, also Brisbane) to monitor the concentration of dangerous gases use for general public. These are able to take advantage of the ad hoc wireless links rather than wired installations, which also make them other mobile use for testing readings in dissimilar areas.

4. SIMULATION AND PERFORMANCE ANALYSIS

First, we will discuss the procedures with the highest distribution rate against the procedures having central controlling node. Usually the central controlling node (BS) decreases the complexity of the detection procedures as compared to distributed procedures [7]. But worse problem in centralized procedures is the presence of BS as the error point, which leads to the extreme decrease of the energy of the neighbouring nodes compared to the other nodes networks, with also cause security fear in the network. The next essential scrutiny is the analysis of the deterministic protocols in comparison with non-deterministic procedures. Since of the possibility nature of non-deterministic protocols, attacking be difficult used for any attacker [49]. In deterministic procedures, at the time of performing the protocol, the witness node protocols are considered unchangeable. Thus, if the enemy compromises and replicates a node and is in agreement with the witness nodes of that particular node, it can easily secure any number of the clone nodes. In this condition, the detection protocol is deficient. Then an optimal procedure must be non-deterministic with full distributed (NDFD), so because to detect the clone node in the mobile WSN reliable.

It means Clone attacks into wireless sensor networks determination initiate many insiders attack similar to wormhole or black hole attack via changing the code of the compromised node with replicating it in various part of network. The detection of clone be based on the location claims with it is discussed below. There be two different approaches in detecting a clone into detection of clone in Stationary WSN. They be
1. Centralized approach 2. Distributed approach

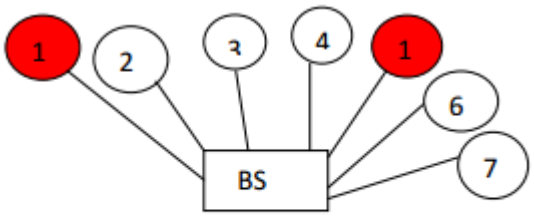
Centralized approach
In this article we have a base station(BS)or a remote sink and this initiates the protocol for detection of clone. All the sensor nodes of the network will report the BS about their location information. And the BS will compare the location claims it has received for finding conflicts. but there exist, two nodes with different location claims then BS will broadcast the revoke message for the entire network. The drawbacks [3] of this approach are • but the BS is drained out of energy, next detection can't be preceded. This will make detection protocol to fail. This is referred as single point failure. • But the adversary compromises the BS, and then the clones will not be detected. • The nodes closest to the BS will contain a high routing load. base on this, if the adversary targets these highly loaded nodes then the detection will fail. • The BS waits used for all sensors near

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

report in addition to then analyse them to recover the conflicting claims. Then floods the network which increases the storage and computation overhead at BS.



Nodes with same id and different locations

Fig. 1 Clone attack

Distributed Approach:

This approach doesn't depend on Base station. The detection of clone is distributed among the sensor nodes in network. The drawbacks of the previous approach are overcome by this distributed approach. There are different protocols that are discussed below under this category.

5. CONCLUSION

A paper all procedures presented used for the detection of imitation node attack in sensor networks by mobile nodes is reviewed and analysis. Also, by using mobility criteria, a new classification for node replica detection procedures and attacker model are proposed. To compare and evaluate different procedures, different metrics are introduced and used for theoretical analysis and classification procedures. Moreover, results of theoretical analysis and metrics are used for assessment procedures. Finally, the theoretical analyses of different approaches are discussed. Analysis results demonstrate to the procedures, based going on location information (UTLSE, MTLSD, and SPRT) contain a higher detection rate with low false alarm rate. But, here be two important notices; initialsuitable to the constraints of WSNs, access location information for all nodes is a strict assumption. Moreover, it can be seen that the energy overhead in this approach is too high. Therefore, regarding the theoretical analysis it can be seen that the SHD largely meets the criteria for a suitable solution and also shows good performance. However SHD energy consumption in large-scale WSNs still is high. Therefore, regarding limitations WSN, to achieve an optimal solution for node replica detection, there is an open area for researchers..

REFERENCES

1. *J.-W. Ho et al," Distributed detection of mobile malicious node attacks in wireless sensor networks", Ad Hoc Networks 10 (2012) 512–523*
2. *W.T. Zhu et al," Detecting node replication attacks in wireless sensor networks: A survey", Journal of Network and Computer Applications 35 (2012) 1022–1034*
3. *S.K.Das et al, "A synopsis on node compromise detection in wireless sensor networks using sequential analysis", Computer Communications 34 (2011) 2003– 2012*
4. *Michael Riecker et al," A Survey on Intrusion Detection in Wireless Sensor Networks", Technical Report, SEEMOO-TR-2011*
5. *V.Manjula et al," Replication attack mitigations for static and mobileWSN" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011*
6. *Ho et al," Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing" IEEE Transactions on Mobile Computing, Vol. 10, No. 6, June 2011*
7. *Roberto Di Pietro et al," Securing Mobile Unattended WSNs against a Mobile Adversary", IEEE 2010*
8. *Chen et al, "Sensor Network Security: A Survey", IEEE Communications Survey & Tutorials. Vol 11, No2, Second Quarter2009*