[Kumar, 3(10): October 2016]
DOI- 10.5281/zenodo.159497

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

MALICIOUS NODE IDENTIFICATION USING THE PROXY SERVER AND QUERY CONDITIONAL MODEL APPROACHES IN THE WIRELESS SENSOR NETWORKS.

Mr. A. Senthil kumar*[1] and Dr. K. Ravikumar[2]
* Department of Computer Science, Karpagam University, Coimbatore
Department of Computer Science, Tamil University, Thanjavur-10.

ABSTRACT

Collection of autonomous computers are referred as Computer Networks consist of various devices that are attached to it and it must needs to be completely secured from inside or outside threats. Threat is an unwanted assault must be mitigated in all the measures by applying various cryptographic algorithms or models. Similarly, an attack is also an important issue to be considered in the networks both in the case of wired or wireless mode of network arrangements. In general Replay Attacks includes the most vulnerable attack in case of wireless networks particularly, Wireless Sensor Networks. The categories of attacks in the section one is followed by the hardware architecture that explains the sensor network arrangement in the section two. The research proposal suggests the query conditional model approach using the proxy server specifications to identify the intruder detection analysis to pinpoint the adversaries where the networks are spoofed by the false IP injection packets in order to compromise the networks. Till date the necessary authentication scheme are applied in the various modes to identify the intruding effect but the applications are subject to vulnerable because of wireless modes. Normally, hacking gets easily applicable in the wireless devices due to the shared nature of the wireless medium, also through modifying the Media Access Control (MAC) address of the network. The issue can be solved by the new proposal of the query conditional model approaches which exactly identifies the intruder and blacklist them in order to quarantine them like a viral scanner tool in the section three. Further the sections depict the pre-implementation procedure to notate the findings and followed by the analysis that narrates the pinpoint inference of the attacks detected and solved. Any sensor nodes that are compromised are arranged through the modular arithmetic fashion but still the deployment is not possible in the initial stage. The existing architectural pattern of the sensor node arrangement is random, but security arrangements are dynamic and it is up to the organization to decide the infrastructural needs. The cost of the node arrangement can also be considered in the feasibility stage. The research proposal and the model are applicable to any Advanced Encryption Standard [AES] algorithms in the near future.

Keywords: *Security, Encryption Standard, Query Model, Sensor, Attacks, Proxy.*

I. INTRODUCTION

According to author Michel Whitman, Information Security is defined as the protection of the computer assets such as the data, hardware and software which are often called as the resources [1]. It can be shared when computer networks are installed and the facility of sharing can be enriched by the use of security implementations over it. Identity attacks are considered to be the most vulnerable attack in networks which compromise the basic operation of the wireless networks, sensor networks in particular. The research paper suggests the importance of the attacks basically in the initial section followed by the architecture of wireless sensor networks. The third section reveals the importance of the query conditional approaches which to identify the exact intrusion by means of the constraint or model specifications [3]. Query conditional approach is suggested as one of the finest techniques used in the recent AES (Advanced Encryption Standard) Procedure for any Public Key Cryptosystems**.** The Section four continues to write the design steps to adopt the sample procedure as any input or the output of a problem is designed basically. The Section five produces the implementation procedure sample and the respective constraints are depicted by the means of notations. Theoretically, Identity attacks are possibly or classified in two stages. One is, ‘Spoofing attacks ‘and the other is ‘Sybil attacks’. William Stallings [3] in his text book suggests IP Spoofing [Internet Protocol] intruders can create false IP address packets and inject them into the network to compromise the network. The original user suspects it as the valid IP and allows the intruder to access the network. Now days, the total IP is compromised by the adversary and the network is vulnerable. The issue is solved in the research proposal by introducing the popular modular arithmetic technique to identify the intruder exactly by monitoring the nodes through the constraints. The existing proposal identifies the network identity attack flaw through the regression and statistical analysis paper [3] but focus on sybil attack notification. Of course Sybil attack is one of the identity based attack but Spoofing is another variant of it. The main focus of this paper suggests to align the nodes of the sensor networking architecture [3] where nodes deployment are arranged in a random fashion [3] but this research paper proposes to limit the network boundary nodes can be arranged in a linear fashion one by one or next to next to identify the intruder or adversary exactly. Other advantages include the proposed system normally advises the public key cryptosystem and also the AES (Advanced Encryption Standard) Procedure to start the ciphering of bits from 128 initially and continue further. The linear arrangement of nodes when applying through the modular arithmetic fashion can be updated to limited nodes initially and can be scaled up to more number of nodes as the organization or the application need in near future.

II. ATTACKS AN OVERVIEW

According to William Stallings, Attacks are defined as an assault especially in the form of a method or technique to evade security services and violate the security policy of a system. Attacks are classified as 1. Passive attacks 2. Active attacks in general. Attempts to learn or make use of information from the system but does not affect the system resources are revealed as 'Passive attacks'. An active attack attempts to alter the system resources or affecting its operation from its original working stage is known as 'Active attack.' In other words, a passive attack in the computing security is an attack characterized by the attacker listening on communication. It is characterized as the attacker listening in on communication. In such an attack, the intruder/hacker does not attempt to break the system or otherwise change data. Passive attacks basically mean that the attacker is eavesdropping. This is in comparison to an active attack, where the intruder attempts to break into the system. Even though a passive attack sounds less harmful, the damage in the end is just as severe if the right type of information is obtained. An active attack, in computing security, is an attack characterized by the attacker attempting to break into the system. During an active attack, the intruder will introduce the data to the system as well as potentially change the data within the system. An active attack is commonly referred as 'hacking.' Comparing it to a passive attack where the intruder listens on communications. An example of an active attack is a 'Denial of Service (DOS) attack. The focus of identifying passive attacks is highly difficult, but using the cryptographic techniques solves the issue of impersonating or data reading. The issue is solved by using "Cryptographic algorithms'' such as Diffie-hellman, RSA, Elliptic curve etc. The following figure -1 depicts passive attack with its type namely the 'Release of message contents '

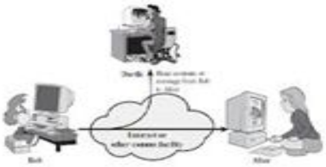

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Figure – 1 Passive attack

This comes under the passive attack and where the contents are released during the transfer and the next fig-2 depicts the denial of service where the intruder disrupts the service where the intruder evades the services of the server and the server becomes a non-responsive.

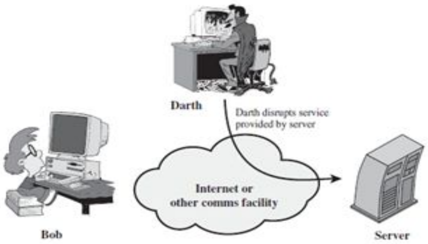

Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Figure – 2 Active attack

The arrangement of nodes in a wireless environment is a heterogeneous since the nodes which are deployed in the ground may have difference in the configurations. So it is necessary to learn the architecture in wireless networks, and sensor nodes in particular. The next section narrates the basic architecture of sensor networks with its sketch.

III. SESNSOR NETWORK ARCHITECTURE

In general, all the sensor networks are described with its various parameters namely the sensor, sensor nodes and the nodes that comprehend the network alias 'Sensor network.' Differentiations between all of these terms are essential to learn for the research proposal because these are a major component that integrates the system. Sensor is defined as a transducer which converts the physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals[4]. The node referred in the network is sensor node and this is basic unit in sensor network that contains on-board sensors, processor, memory, transceiver, and power supply. The total network namely the sensor network consists of a large number of sensor nodes and the nodes deployed either inside or very close to the sensed phenomenon.

Heterogeneous wireless sensor networks are grouped into a large number of wireless devices equipped with different communication and computing capabilities. While comparing with homogeneous wireless sensor networks, where all the devices possess the same communication and computing capability, H-WSNs includes a numerous operating environments [4]. The nodes with its path and its communication established are framed by the support of its architecture as follows

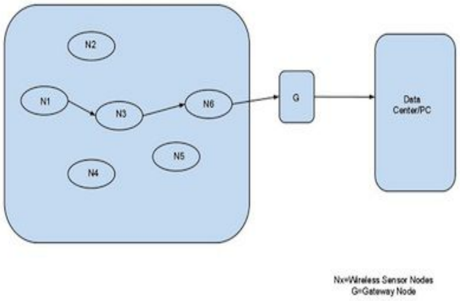


Fig.3. Wireless Sensor Networks Hardware and its Architectural Platform

3.1. Sensor nodes

Sensor nodes are the network components that are sensing and delivering the data. Depending on the routing algorithms used, sensor nodes will initiate transmission according to the measures and/or a query originated from the Task Manager. According to the system application requirements, nodes do some computations [5]. After computations, it passes its data to its neighboring nodes or simply passes the data to the Task Manager. The sensor node act as a source or sink/actuator in the sensor field. The definition of a source is to sense and deliver the desired information. Hence, a source reports the state of the environment. On the other hand, a sink/actuator is a node that is interested in some information a sensor in the network might be able to deliver. As mentioned earlier, the sensor field constitutes sensor nodes. Typically, a sensor node can perform tasks like computation of data, storage of data, communication of data and sensing/actuation of data. A basic sensor node typically comprises of five main components and they are namely controller, memory, sensors and actuators, communication device and power supply. A controller is to process all the relevant data, capable of executing arbitrary code. Memory is used to store the programs and intermediate data. Sensors and actuators are the actual interface to the physical world. These devices observe or control physical parameters of the environment. The communication device sends and receives information over a wireless channel. And finally, the power supply is necessary to provide the energy. In wireless sensor networks, power consumption efficiency is one of the most important design considerations[6]. Therefore, these intertwined components have to operate and balance the trade-offs between as small energy consumption as possible and also the need to fulfil their tasks.

3.2 Gateways

Gateways allow the scientists/system managers to interface the Motes to personal computers (PCs), personal digital assistants (PDAs), Internet and existing networks and protocols. In a nutshell, gateways act as a proxy for the sensor network on the Internet. Gateways can be classified as active, passive, and hybrid. Active gateway allows the sensor nodes to actively send its data to the gateway server. Passive gateway operates by sending a request to sensor nodes. Hybrid gateway combines capabilities of the active and passive gateways.

3.3 Task Managers

The Task Manager will connect to the gateways via some media like Internet or satellite link. Task Managers comprise of the data service and the client data browsing and processing. These Task Managers can be visualized as the information retrieval and processing platform. All information (raw, filtered, processed) data coming from sensor nodes is stored in the task managers for analysis. Users can use any display interface (i.e. PDA, computers) to retrieve or analyze these information locally or remotely.

IV. QUERY CONDITIONAL MODAL

In general, the number of query messages routed by a node say n1, is incremented whenever the controlling node receives a query message from node n1 in which the noted value is less than the fixed max value for the transmission. The Queries originating from one node say n1 are not counted; only the Queries originated at somewhere else and routed by another node say x or y will be counted. Node P are counted. The controlling node here turns into as a proxy server decides if the Query was originated by the controlled node or not by looking at the noted value. If the node n1 has originated the Query, then the Query message would have a noted value equal to the fixed max value allocated. To add, the number of Query messages routed towards node n1, is incremented whenever the controlling node sends a Query message to the controlled node n1. Both the Query messages originated at the controlling node and the Query messages just forwarded by the controlled node are counted. In addition, the number of Query Hit messages submitted by node P, is incremented whenever the controlling node receives a Query Hit message from node P . The message must be originated (not forwarded) by node P. The controlling node can decide this by looking at the IP address field of the message, which stores the IP address of the originator of the message. The number of Query Hit messages routed by node P, is incremented whenever the controlling node receives a Query Hit message from node P in which the IP Address field in the message contains an IP address different than that of the node P. Query Hit messages originating at node P are not counted. The number of Query Hit messages satisfying queries of node P, is incremented whenever a Query message formerly submitted by node P receives a Query Hit through or from the controlling node. To observe this, whenever the controlling node receives a Query message whose noted value is the fixed max secured value , it records in its internal table (using the message ID of the Query message) that the Query originated from the neighbor P. Then, after receiving a Query-Hit message with the same message ID, the controlling node decides that the Query Hit message is for that controlled neighbor and increments the counter hqsn1. The controlling node counts only once for all the Query Hit messages received for the same query. Satn1**:** Whenever a node is satisfied with the service provided by the node P, SerQHn1 will be incremented. To find whether the node has been satisfied with the transaction, the node who received the service returns a feedback packet to the controlling node which controls the node P or broadcasting can also be done about the satisfaction it received from the node if any problem in the network. The values of these counters indicate both whether the neighbor is a free from the malicious or intrusion.

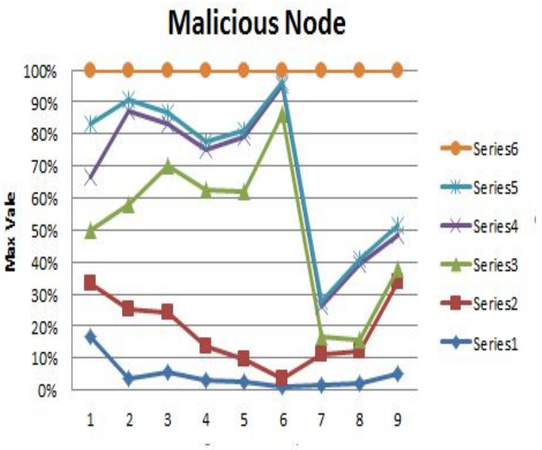


Fig – 1 Node Detection with Secured Values Fixation

V. PROCEDURE & IMPLIMENTATION

The above research proposal is implemented in Netbeans IDE[ ] integrated with all java components. The IDE consists of built-in packages for the networks and security methods to incorporate the user requirements dynamically. To specify the proposals, the following procedure includes the parameters and rule to implement in a readymade fashion.

Procedure node deployment (x1, x2, x3) where x1, x2 and x3 represents sample nodes

```
{
Initialized x1 = 1; x2= 0; x3 = 0;
Assign key value for the node x1 say x1 = k1 && x2 = k2 && x3 = k3 ¥ x1…xn;
N1 = 1345.23; n2 = 6934.56; n3 = 4972.01;
Ap1 = r1; ap2 = r2; ap3 = r3; ap4 = r4;
qk ∧ x1 ∧ k1 ∧ n1 ∧ ap1 =  1 ¥ x1 <qk && x1 <= (q+1)k;
}
Procedure threat occur(x1, k1, n1, ap1)
{
Let a1 = t1;
If (x1(a) = = 1)
{
Call node deployment(x1)
{
N1 = 1345.23;
While (x1 = = n1 && x1 = = ap1)
{
        x1 = k1;
        x1 = n1 &&  ap1 = 1;
        display ( x1 (a)) ;
        x1++;
        }
        else ignore (x1(a) = =1);
        }
```

```
Repeat threat occur(x2, k2, n2, ap2);
}
Procedure threat occur(x1, k1, n1, ap1)  // for node2
{
Let a1 = t1;
If (x1(a) = = 1)
{
Call node deployment(x1)
{
N1 = 1345.23;
While (x1 = = n1 && x1 = = ap1)
{
            x1 = k1;
            x1 = n1 &&  ap1 = 1;
            display ( x1 (a)) ;
            x1++;
            }
            else ignore (x1(a) = =1);
            }
Repeat threat occur( ); }
Procedure Rectify Replay Attack(int x1,x2, int n1, int rf1,rf2)
{
If (x1 >> n1 || x2 >> n2)
Display ("Node Over routes the Query Conditioned Value and Subject to Hack");
else
do   {
Rf1 = x1 || x2 || x3 enum [0.1,0.2,0.3 … 1.0]
X1 = 1;
If x1 = = rf1 (0.1 || 0.2 || 0.3 || 0.4….1.0)  && x1 = n1
{
Display ("Node 1 which is 'x1' is free from replay attacks and is in safe state");
Else
Display ("Node 1 is unsecured and subject to hack since un holding the secured values or nonce values");
End Procedure;
```

VI. PERFORMANCE ANALYSIS

According to the National Institute of Standards and Technology [NIST], [2] fixed standard secured values to any particular security mechanisms. The value which is assigned is used as an access monitoring capabilities that turn on security issues and also which overrules the values. The following sketch arranges the nodes and the values in the horizontal axes and increases the security concerns in the vertical column. The mapping of each co-ordinate corresponds to the method of the information secured in the network with suitable implementations.

The code is implemented in JAVA Net beans IDE framework and can be scalable to upward compatibility in near future. In this research proposal, assignment of nonce values and secured value initializes at the beginning and proceeds for data transmission over the networks. According to the definition of replay attacks, 'repeating previous known values' [3] and guessing the common resource in a network is easily executed by a hacker. The research proposal addresses the issue by assigning suitable secured values which is suggested for each node along with the nonce value randomly, so that any node which overruns the nonce value and the secured value is subjected to be hacked. It is detected easily by executing the implementation code in the respective node and coining the system by both the secured parameterized values.

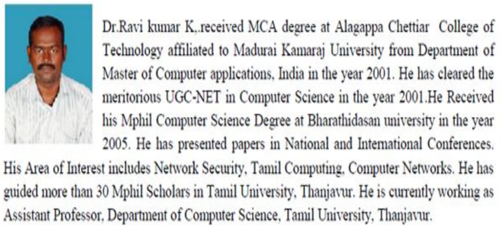
VII. CONCLUSION

The need of secured rules is one of the mandatory suggestions for any application that are executed in the networks. Hence the new rule conditioning the security parameters is a welcomed approach day by day. One of the finest techniques implemented in this approach is the nonce based rule and modular arithmetic approach that exactly detects and locates the intruding activities and overcomes the intrusion. The respected model not only suggests the activities intrusion but also coins the need of security in the AES applications. Any application which runs in the sensor networking routes, the application in a linear fashion which cannot be routed in a Wireless Environments where signals and deployment is not done linearly, but the intention of doing linear based approach can be scaled to randomized arrangement of nodes can be done currently and also in future.Initially the secured rule parameterized approach can be executed to the limited nodes and can be updated to more number of nodes as decided by any organization. Thus any application which runs over the wireless networks can be easily secured by detecting the replay attacks and can be overwhelmed by implementing this research fact.

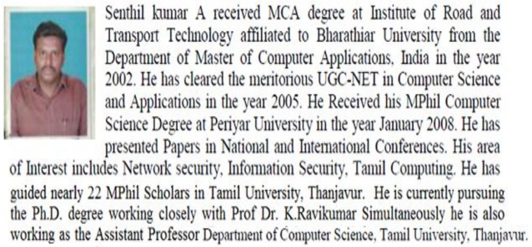
REFERENCES

1. *"Computer Networks" Andrew S Tanenbaum, Fourth Edition, Pearson Education Inc Copyright 2003.*
2. *"Principles and Practices of Information Security", Dr.Michael E.Whitman, CISM, CISSP and Herbert J.Mattord, CISM, CISSP, © 2009 by Course Technology a Part of Cengage Learning.*
3. *"Cryptography and Network Security", Principles and Practices, William Stallings, Fourth Edition", Copyright © 2006, by Pearson Education, Inc.*
4. *"A Wireless Embedded Sensor Architecture for System-Level Optimization", J. Hill and D. Culler, Technical Report, U.C. Berkeley, 2001.*
5. *A. Krishnakumar and P. Krishnan, "On the accuracy of signal-strengthbased location Estimation techniques," in Proc. IEEE INFOCOM, Mar. 2005, pp. 642–650.*
6. *Perrig, A., et al., SPINS: Security protocols for sensor networks. Proceedings of MOBICOM, 2001, 2002.*
7. *B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in Mobile ad hoc networks," in Proc. 19th IEEE IPDPS, 2005, p. 288a.*
8. *A. Wool, "Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation," Wireless Netw., vol. 11, no. 6, pp. 677–686, Nov. 2005.*
9. *T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, IETF, 2005.*
10. *R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February1978.*

BIBLIOGRAPHY



Dr.Ravi kumar K,.received MCA degree at Alagappa Chettiar College of Technology affiliated to Madurai Kamaraj University from Department of Master of Computer applications, India in the year 2001. He has cleared the meritorious UGC-NET in Computer Science in the year 2001.He Received his Mphil Computer Science Degree at Bharathidasan university in the year 2005. He has presented papers in National and International Conferences. His Area of Interest includes Network Security, Tamil Computing, Computer Networks. He has guided more than 30 Mphil Scholars in Tamil University, Thanjavur. He is currently working as Assistant Professor, Department of Computer Science, Tamil University, Thanjavur.



Senthil kumar A received MCA degree at Institute of Road and Transport Technology affiliated to Bharathiar University from the Department of Master of Computer Applications, India in the year 2002. He has cleared the meritorious UGC-NET in Computer Science and Applications in the year 2005. He Received his MPhil Computer Science Degree at Periyar University in the year January 2008. He has presented Papers in National and International Conferences. His area of Interest includes Network security, Information Security, Tamil Computing. He has guided nearly 22 MPhil Scholars in Tamil University, Thanjavur. He is currently pursuing the Ph.D. degree working closely with Prof Dr. K.Ravikumar Simultaneously he is also working as the Assistant Professor Department of Computer Science, Tamil University, Thanjavur.