International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 7 (October '2015)

DETECT AND LOCALIZE REPLAY ATTACKS IN WIRELESS SENSOR NETWORKS USING MODULAR ARITHMETIC CONSTRAINTS AND NONCE STANDARDIZATION RULES

A.Senthilkumar,
Assistant Professor,
Department of Computer Science,
Tamil University, Thanjavur

K.Ravikumar,
Assistant Professor,
Department of Computer Science,
Tamil University, Thanjavur

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

Keywords: Replay attacks, Modular Arithmetic, Sensor Networks, Threat, Nonce

I.INTRODUCTION

According to author Michel Whitman, Information Security is defined as the protection of computer assets such as the data, hardware and software which very 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 where they will compromise the basic operation of wireless networks, sensor networks in particular. This research paper suggests the importance of attacks basically in the initial section followed by the architecture of wireless sensor networks. The third section reveals the importance of modular arithmetic methodology where to identify the exact intrusion by means of the constraint or model specifications [3]. Modular arithmetic is one of the finest techniques used in recent AES (Advanced Encryption Standard) Procedure that too for any Public key cryptosystems. 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. Section five produces the implementation procedure sample where the respective constraints are depicted by 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] where 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 a time, the total IP is compromised by the adversary and the network is vulnerable. This issue can be solved in this research proposal by introducing the popular modular arithmetic technique to identify the intruder exactly by means of monitoring the nodes through the constraints. The existing proposal identifies the network identity attack flaw through regression and statistical analysis paper [3] but focuses 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 [Ref 3 – paper] 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 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 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 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 into 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 can be 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 data into the system as well as potentially change data within the system. An active attack is what is commonly thought of when it is referred as 'hacking'. Comparing it to a passive attack is where the intruder listens in 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 can solve the issue of impersonating or data reading. The issue can be 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 '

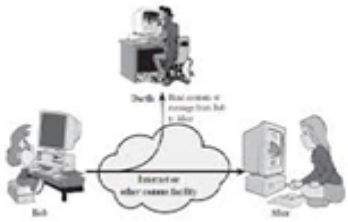


Figure 1: Passive attack

this comes under the passive attack and where the contents are released while in transfer and the next figure 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 non-responsive.

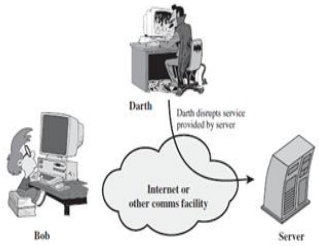


Figure 2: Active attack

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

III.SENSOR NETWORKS ARCHITECTURE

In general, any sensor networks can be 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 this research proposal as 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

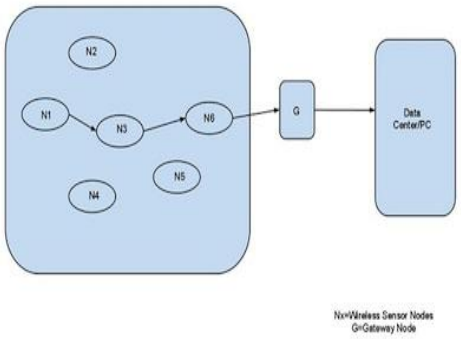


Figure 3: Wireless Sensor Networks Hardware and its Architectural Platform

a) Sensor nodes

Sensor nodes are the network components that will be sensing and delivering the data. Depending on the routing algorithms used, sensor nodes will initiate transmission according to measures and/or a query originated from the Task Manager. According to the system application requirements, nodes may do some computations [5]. After computations, it can pass its data to its neighboring nodes or simply pass the data as it is to the Task Manager. The sensor node can 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 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 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 fulfill their tasks.

b) Gateways

Gateways allow the scientists/system managers to interface 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.

c) Task Managers

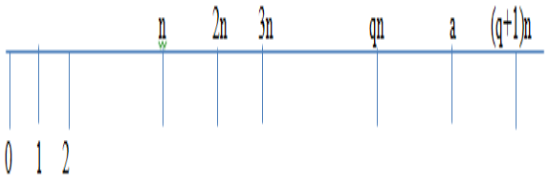
The Task Manager will connect to the gateways via some media like Internet or satellite link. Task Managers comprise of data service and client data browsing and processing. These Task Managers can be visualized as the information retrieval and processing platform. All information (raw, filtered, processed) 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.MODULAR ARITHMETIC METHODOLOGY

The research proposal initiates the arrangement of sensor nodes with reference to the context, "modular arithmetic methodology"[3]. In general, methodology deals with systematic, theoretical analysis of the body of the methods applied to a field of study, or the theoretical analysis of the body of the methods and principles associated with a branch of knowledge. It, typically encompasses concepts such as paradigm, theoretical model phases and quantitative, qualitative techniques. A methodology does not set out to provide solutions but offers the theoretical underpinning for understanding which methods, set of methods or so called "best practices" can be applied to a specific case. To suggest this approach, this model uses the modular arithmetic methodology to make the sensor nodes arrangement in a linear fashion which is highly difficult to represent. The model defines, given any positive integer 'n' and any nonnegative integer a, if we divide 'a' by 'n', we get an integer quotient 'q' and an integer remainder 'r' that obey the following

$a = qn + r$ - Equation - 1

where 0 r < n; q = a/n where x is the largest integer less than or equal to 'x' . the relationship a = qn + r, 0<r<n is represented diagrammatically as follows



a) Description

The methodology suggests, given 'a' and positive 'n', it is always possible to find 'q' and 'r'. that sasify the preceding equation – 1. Here the integers are represented on the number line. The condition is 'a' will fall somewhere on that line. Starting at '0', we can proceed to 'n', '2n', upto 'qn' such that 'qn<- a' and '(q+1) n>a'. The distance from 'qn' to 'a' is 'r' and we can found the uniqe values of q and r. The remainder 'r' is often referred to as a residue. This situation implies the use of modular arithmetic which divides and obtains the occurance of any positive integer must hold in between the two end points. If the condition overlooks the specification 'a'we can represent the the integer value goes larger than the fixed values. The next subsection corelates the methodology, modular arithmetic into arrangement of nodes and the attacks that work on the nodes can be depicted with the rule fixed in the nodes and that bypasses the rule.

V. THREAT IDENTIFICATION AND MITIGATION

In the arrangement of nodes that are numbered from 0 , 1, 2 and upto the network boundary say k with the limitation are installed as sensors that is deployed initially in a linear fashion. The nodes that runs any object say 'o' can be assigned unique value to be fixed initially can be dynamically altered according to the application needs. In the initial node, say '0' we can frame the object 'ob' at '0' where the object represents the nonce which may be a timestamp, a counter, or a random number ; the minimum requirement is that it differs with each request. The nodes can proceed upto k, 2k upto qk such that qk<= a where 'a' is the key assigned based on AES which is a nonce to fix in the key. The last node depoloyed must lie between the framing of all possible values. If the node say (q+1)k >= a which means, the node value in which the key values assigned crosses the limit of nonce value arrangement say [0..45], we can strongly believe that threats may occur if the nodes deployed crosses the linear arrangement.

The deployment of nodes can be represented in the following figure – as

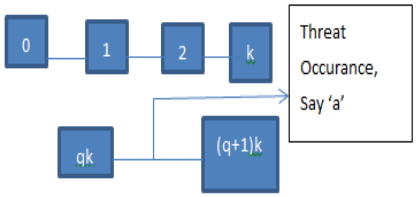


Figure 5: Node Deployments and Threat Occurance

The nonce values along with the key can be transmitted in the transaction that occurs between the nodes. The nonce value with matching of the object value say ob must be equally depicted in all the nodes which is noted as "ob" here. If the value unequally occurs in any of the nodes or if the nodes crosses the limit of deployment may subject to get hacked by the intruders. Hence, the nodes must be strictly adhered to follow the modular arithmetic fashion with deployments and must follow the rules adapted. the advantage of this technique hold two benefits. Different nodes can be arranged according to the organizational needs, but this approach follows the sequential arrangement , so attack must occur in the sequential way only and not to take place in random way primarily. In the secondary way, the nonce value and key assignent is dynamic and is computed for every arrangement of nodes uniquely in a linear fashion. Once the network crosses the limitation we can suggest the threat occurance and subject to hacking. This can be avoided by framing the limitations. The next section follows the pseudocode and provides implementaion idea to the methodology and design specified in this research proposal.

VI.PROCEDURE AND IMPLEMENTATION

The above research proposal is implemented in Netbeans IDE integrated with all java components. The IDE consists of built-in packages for networks and security methods to incorporate 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 keyvalue 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 threatoccur(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 threatoccur(x2, k2, n2, ap2);
}
Procedure threatoccur(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 threatoccur();}
Procedure RectifyReplayAttack(int x1,x2, int n1, int rf1,rf2)
{
 If (x1 >> n1 || x2 >> n2)
 Display ("Node Overroutes the Nonce 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 unholding the secured values or nonce values");
End Procedure;
```

VII. PERFORMANCE ANALYSIS

According to National Institute of Standards and Technology [NIST], [2] fixed standard secured values to any particular security mechanisms. The value which is assigned can be 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 increase of security concerns in the vertical column. The mapping of each co-ordinate corresponds to the method of information secured in the network with suitable implementations.

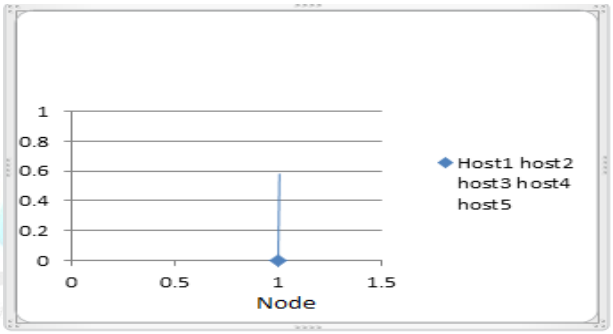


Figure 6: Node Initialization with Nonce and Secured Values

The code is implemented in JAVA Netbeans IDE framework and can be scalble 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 can be easily executed by a hacker. This research proposal addresses the issue by assigning suitable secured values suggested for each node along with nonce value randomly, so that any node which overruns the nonce value and the secured value is subjected to be hacked. This can be detected easily by executing the implementation code in the respective node and coining the system by both the secured parameterized values.

VIII.CONCLUSION

The need of secured rules is one of the mandatory suggestions for any application that are executed in networks. Hence new

rule conditioning the security parameters is a welcomed approach day by day. One of the finest techniques implemented in this approach is nonce based rule and modular arithmetic approach that exactly detects and locates the intruding activates and overcomes the intrusion by applying this rule. The respected model not only suggests the activities intrusion but also coins the need of security in AES applications. Any application which runs in sensor networking routes the application in a Lineared fashion which cannot be routed in a Wireless environments where signals and deployment could not be 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 this secured rule parametized approach can be executed to 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.

IX.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 andPublic-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February1978.