INTRUSION DETECTION AND AUTHENTIC IDENTIFICATIONS THROUGH THE KEYS –DISCLOSURE APPROACH IN THE WIRELESS SENSOR NETWORKS

A.Senthil kumar,
Research Scholar (Ph.D-PT) in Computer Science,
Karpagam University,
Coimbatore, India.

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

Abstract: In general, Networks are defined as the interconnection of the autonomous computers in which its advantages widespread its service primitives, topologies, types, bandwidth and major classifications like wired or wireless streams. The method is to include and disseminate applications in the wireless networks is an essential talk today. To add advantage, Wireless Sensor Networks emerge to help the increased applications to run on. Web services and Web applications that run on the Internet enabled technologies need to safeguard from various threats. The problem of identifying the intrusions, preventing further and protecting an everlasting focus is needed today to run particular applications in an immortal way. In this approach, key-disposition approaches in various pathway whether one-way, two-way or in a multi-way mechanisms are analysed in the proposed work that finds the application to scrutinize effectively with the implementations. The inference shows that the proposed parameter value with its key notations includes the benefits and increases the security policies to adapt in the various internet applications regard to the wireless sensor networks based on authentication schemes.

Keywords: Sensor Network, Authentication, Key-Disclosure, Routing, Web-Applications, Clusters, Packets, Secret Key.

I. INTRODUCTION

Networks are well suitable to run, and share any type of applications ranging from small to large internet applications. The increase in the bandwidth to wireless mode is very essential need for the generations. The mode to increase its configuration categorized as wired or wireless depends on the organization which implements their own or other applications. But the extent they are secure and prioritized with the adaptive scalability is the major issue to approach. The research work starts with the literature on the wireless sensor networks with its parameters, followed by the architecture to implement the scheme. A section of key-disposition approach is applied to enrich the security features. The model of the one-way analysis, two-way analysis and multi-way analysis are strongly categorized with its necessary advantages by adding the proposed system stronger to run any type of internet, web applications. The range of the systems includes the wireless environments like padding mobile, laptops, and tablets and so on. The sample procedure written in the proposal delivers key note notations which are utilized for the source code. The inference and the parametric value adapted in the work normally address is the security issue with its previous notations. The value to be adapted strictly adheres all security policies. The apprehension in the authorizations and its facilities are very well executed by its authentication schemes. The model also shows to increase further number of clients in addition with respect to its robustness. Internet based web-applications are added in the each concepts that normally enriches security features and parameters existing in the network.

II. LITERATURE ON WIRELESS SENSOR NETWORKS AND ITS VULNERABLE ISSUES

The WSN is a built of "nodes" – from a few to several hundreds or even thousands, where each node is connected with one (or sometimes several) sensors. Each such sensor network node typically has several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The topology of the WSNs varies from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. However, while the routing strategies and wireless sensor network modelling are getting much preference, the security issues are yet to receive an extensive focus. Most of the threats and attacks against the security in the wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, the wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to the security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In the most of the cases various security issues and the threats related to those and are considered for the wireless ad hoc networksand are also applicable for wireless sensor networks. Attacks against wireless sensor networks are broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Denial of Service (DoS)is produced by the unintentional failure of nodes or malicious action. The simplest Denial of Service (DoS) attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents the legitimate network users from accessing the services or resources to which they are entitled. In a sensor network, sensors monitor the changes of the specific parameters or values and report to the sink according to the requirement. While sending the report, the information in the transit may be altered, spoofed, replayed again or vanished. As the wireless communication is vulnerable to the eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they use distribution of the subtasks and redundancy of information. In such a situation, a node pretends to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack. Wormhole attack is a significant threat to the wireless sensor networks, because; this sort of attack does not require compromising sensor in the network rather, it could be performed even in the initial phase when the sensors start to discover the neighbouring information.

III. ARCHITECTURAL PITCH

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

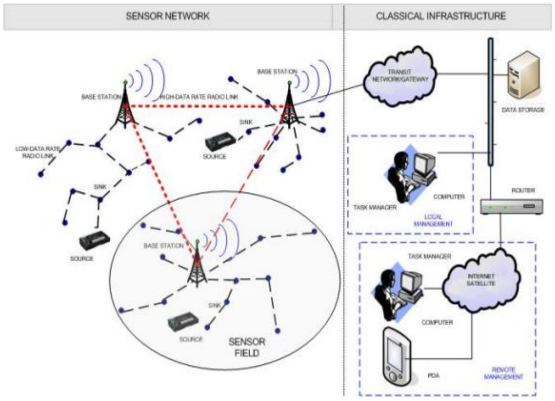


Figure 1: Wireless Sensor Networks Hardware and its Architectural Platform

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 initiate the transmission according to a measures and/or a query originated from the Task Manager. According to the system application requirements, nodes may do some computations. After computations, it passes its data to its neighbouring nodes or simply passes 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 performs tasks like computation of the data, storage of the data, communication of the data and sensing/actuation of data. A basic sensor node typically comprises the 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 the 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 the 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 the wireless sensor networks, power consumption efficiency is one of the most important design considerations. Therefore, these intertwined components have to operate and balance the trade-offs between the 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 the personal computers (PCs), the personal digital assistants (PDAs), the Internet and existing networks and protocols. In a nutshell, gateways act as a proxy for the sensor network on the Internet. Gateways are classified as active, passive, and hybrid. Active gateway allows the sensor nodes to run actively its data to the gateway server. Passive gateway operates by sending a request to the sensor nodes. Hybrid gateway combines capabilities of the active and passive gateways.

3.3 Task Managers

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

3.4. System Components and Operations in a Wireless Sensor Network Communication Architecture

The components and operations between the sensor nodes within the sensor field are explored. It first describes the wireless sensor network architecture and the communication protocols for the wireless sensor network. It is essential to understand the hardware and software level for the power savings strategies. One of the intension of the report is to provide a survey of the sensor nodes in literature and recommend the appropriate hardware based on the specific application.

IV. KEY-DISCLOSURE APPROACH

In every arrangement of the nodes, each sensing node chooses a new authentication key notated as 'Sec-key' to authenticate its reports or any application connected to it. To facilitate verification of the forwarding nodes, the sensing nodes disclose their 'sec-key' at the end of each round. Meanwhile, to prevent the forwarding nodes from abusing the disclosed keys, a forwarding node as, 'fn' can receive the disclosed secret keys, only after its upstream node as, 'un' overhears that it has already broadcast the report or the application, as 'an'. Receiving the disclosed keys, each forwarding node verifies the reports, and informs its next-hop nodeas 'hn', to forward or drop the reports based on the verification result. If the reports are valid, say 'vd'. It discloses the keys to its next-hop node after overhearing. The processes of verification subject to the secret key hold, application tagged with secret key, overhearing, and key disclosure are repeated by the forwarding nodes at every hop until the reports are dropped or the application is delivered to the base station. The key-disposition approach is executed by three levels. In the first level, each node is preloaded with a distinct private key ('pk') from which it can generate a hash chain of its secret keys. In the second level, the cluster – head disseminates each node's at first the secretkey to the forwarding nodes, which filters the false reports later. In the third or termination level, each forwarding node verifies the reports using the disclosed secret keys and disseminated ones. If the reports are valid, the forwarding node discloses the secret keys to its next – hop node after overhearing that node's broadcast. Otherwise, it informs the next-hop node to drop the invalid reports. The process is repeated by every forwarding node until the reports are dropped or delivered to the base station. The different level execution is represented by its flow diagram as figure – 2

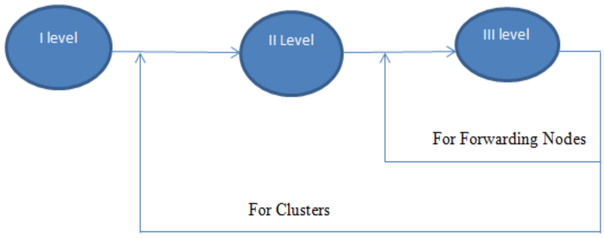


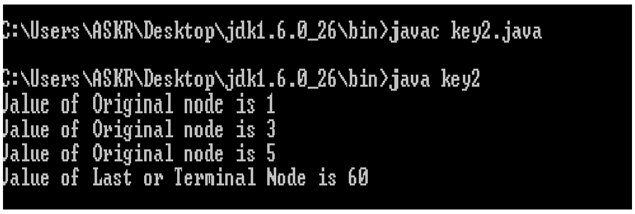
Figure-2 – Different Execution Levels

V.SAMPLE PROCEDURE

```
1.  INPUT: Integer  n and a set of forwarding nodes fn
2.  OUPUT: A Set of application execution R.
3.  R ← $\phi$(empty set)
4.  an ← {xyz &&mnp ϵ V }
5.  Define the Secret Key of Each node i.e x1 ϵ $S_k$
6.  Compute C ← ($S_{k}$ , $A_k$)
7.  Compute Next Hop say fn ← ($S_{k}$ , $A_k$)
8.  Place the Next Node with C || nexthop
9.  Call $S_k$with xyz || mnp ϵ V i.e C ← $S_k$&& xyz ||
    $S_k$&&mnp
10. Repeat Step 9 with Authentic Key , '$A_k$'
11. Compute C ← $S_{k,}$ $A_k$|| ¥ xyz and  ¥ mnp
12. Execute Step 10 for which node until the terminal node
    say, tn completes its report or its application.
```

VI. OUTPUT

The screen display shows the nodes starting from '1' to the next original node identified   by the network which is '3' and further '5'. The display clearly shows the end of the network or the last node which is termed here as '60'



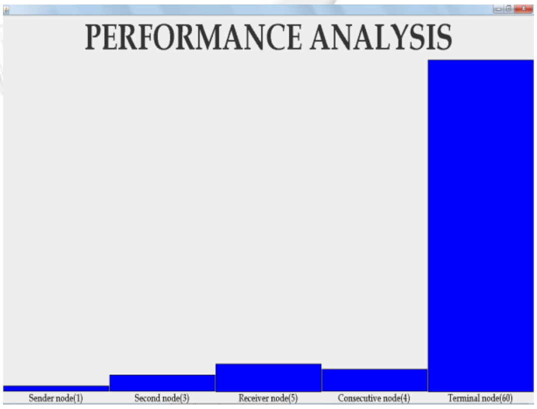
```
C:\Users\ASKR\Desktop\jdk1.6.0_26\bin>javac key2.java

C:\Users\ASKR\Desktop\jdk1.6.0_26\bin>java key2
Value of Original node is 1
Value of Original node is 3
Value of Original node is 5
Value of Last or Terminal Node is 60
```

Screenshot 1 – Node Creations and Application Termination

VII. INFERENCE

The following graph depicts the performance of the key and the work shared in its entire network configuration. The performance shows that the value with its initial assignment, forwarded node and to its next hop and with all of its hops vary from one to another.



Figure– 3 Metrics

VIII.CONCLUSION

The research paper directs the importance of the key usage such as secret key and authentication key through its verifying identities, which are sender node, and next hop node to all other nodes. The work or any application runs on its own provision suggesting that its key value must be completely shared with all of its parameters. The section headings coin the work of security involved with key usage and reporting it through any application. As Internet and e-commerce work is progressing through online and enriching the customer need by running in their own hands , their own authenticity by sharing all of the entities through which their handheld devices may subject to hacking. The hacking activity can be monitored and charged with alarming to enlighten their security needs by running a secret key approach paradigm. The paper hopes the need to fulfil thesecurity needs in the field of Networks of its security implementations.

REFERENCES

[1] Computer Networks, by Andrew S.Tanenbaum, Fourth Edition, PHI Publications, 2009

[2] Cryptography and Network Security, William Stallings, PHI Publications, Sixth Impression 2008

[3] A. K. M. N. Sakib and M. S. Kowsar, "Shared Key Vulnerability in IEEE 802 .16e : Analysis & Solution," presented at the 13th International Conference on computer and Information TechnologyEngineering and Technology, bangladesh, 2010.

[4] R. K. Jha and U. D. Dalal, "A Journey on WiMAX and its Security Issues," Journal of Computer Science and Information Technologies, vol. 1, pp. 256-263, 2010.

[5] M. Bogdanoski, P. Latkoski, A. Risteski, and B. Popovski, "IEEE 802 . 16 Security Issues A Survey," presented at the 16th Telecommunications Forum (TELFOR 2008) Belgrade, Serbia,2008.

[6] 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, February 1978

[7] X. L. Li, F. T. Wen, S. J. Cui, A new cross-realm client-to-client password-authentication key exchage protocol, Journal of Computational Information Systems 2010; 6(13): 4553 – 4561.

[8] W. J. Tsaur, C. C. Wu, W. B. Lee, A flexible user authentication for multi-server internet services, Networking-JCN2001LNCS, vol. 2093, Springer-Verlag. 2001, pp: 174 – 183.

[9] L. Li, I. lin, M. Hwang, A remote password authentication scheme for multiserver architecture using neural networks, IEEE Trans on Neural Network 2001; 12(6): 1498 – 1504.

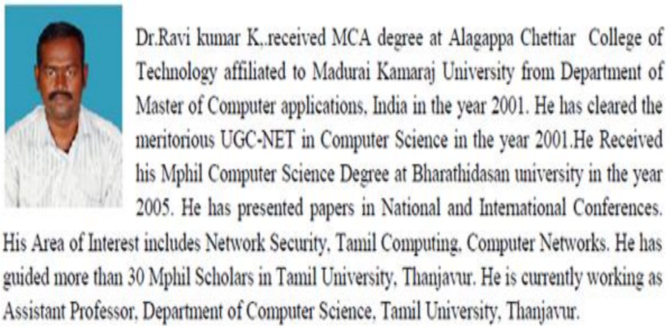
[10] W. S. Juang, Efficient multi-server password authenticated key agreement using smart cards, IEEE Trans on Consumer Electronics 2004; 50(1): 251 – 255.

[11] C. Chang, J. S. Lee, An efficient and secure multi-server password authentication scheme using smart cards, In: Proceedings of the international conference on cyber worlds, November 2004, p. 417 – 422.

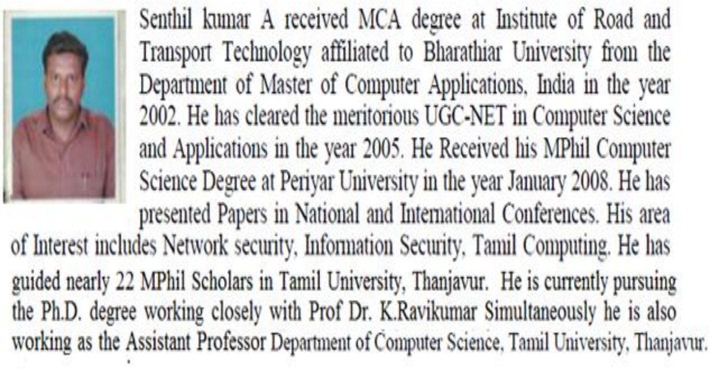
[12] J. L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, Computers & Security 2008; 27(3-4): 115 – 121.

[13] Y. P. Liao, S. S. Wang, A secure dynamic ID based remote user authentication scheme for multi- server environment, Computer Standards & Interface 2009; 19(1): 13 – 22.

AUTHORS PROFILE



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.