International Journal of Technology in Computer Science & Engineering

ISSN 2349 – 1582

Volume 4, No 2, June 2017

Virus Threat Identification in WSN based Networks

S.Natarajan[1]

(Research Scholar,Manonmaniam Sundaranar University,Tirunelveli,TN,India

sivnatarajan@gmail.com)

Dr.H.Abdul Rauf [2]

(Professor & Dean Sree Sastha Institute of Engineering and Technology, Chennai,TN,India

harauf@gmail.com)

Dr.S.P.Victor[3]

(Dean of Science and Associate Professor,St.Xavier's College,Palayamkottai,TN ,Indria)

Abstract: Nowadays Wireless sensor Networks (WSN) are growing rapidly as plenty of applications have been using WSN. Security is a great challenging task in wireless sensor networks. Sensor networks are also used in very sensitive applications like healthcare, military, education, communication, etc. Due to the distributed nature, multi-hop communications and their deployment in remote areas, WSNs are vulnerable to numerous security threats. There are currently various approaches in wireless sensor networks security. In this paper we proposed a new methodology to identify threats due to virus and such malicious codes in WSN

Keywords: Virus, Worm Malware, Signature, DetectionMechanism, Network attacks, security issues, threat models, wireless sensor networks.

1 Introduction

A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to supportively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, etc., at different locations. The development of WSN was originally motivated by military applications such as battlefield surveillance. It also processes the collected data and effectively route them to the nearest sink or gateway node [7]. It consists of a large number of densely deployed sensor nodes. Each node in the sensor network may consists of one or more sensors, a low power radio, portable power supply, and possibly localization hardware such as a GPS (Global Positioning System) unit or a ranging device. These nodes incorporate wireless transceivers so that communication and networking are enabled. In a wireless network, traffic classification and unknown flow detection methods are used to solve the networking issues such as security, congestion, intrusion detection and quality of service [1]. WSNs and internet are integrated as a new application area called Internet of Things (IoT), covering almost every area in daily life. Indeed wireless sensor networks gaining rapid popularity because of their potentially low cost solutions to a variety of real-world challenges [2]. Security in WSNs is not so easy when compared with conventional desktop computers as WSNs have constraints [2] like limitations in processing power, storage, channel bandwidth, energy, etc.

A general wireless sensor network is composed of a number of sensing units or sensor nodes equipped with the appropriate sensors. A sensor field here is referred as the area in which the sensor nodes are placed. A target node is the sensor node which is the source of the information. Sensor nodes are the heart of the network [3]. They are in charge of collecting data and routing this information back to a sink. A sink is a sensor node which is deployed for fulfilment of the sole purpose of receiving, processing and storing the data from the other sensor nodes and finally transmitting the data to the base station which reduces the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sink nodes are also known as data aggregation points. Base station is a centralized point of control within the network which extracts information from the network and distributes the information back into the network. It also serves as a gateway to other networks. The base station is either a laptop or a workstation. Operations of WSN involve communication between sensor nodes and base station. Each of the sensor node senses environment within its reach, performs some computation (if required) and reports

the gathered information to the base station through the sink node. Base station can also be connected with some actuator which will then trigger the alarm for human intervention in case of an event of interest.

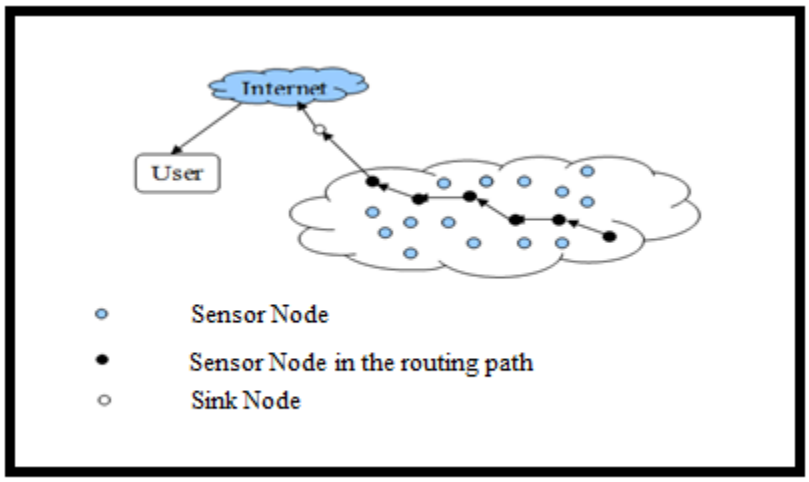

Figure 1: General structure of a wireless sensor network.

.A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices have to overcome the constraints like limitation in their energy, computation power, etc. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attacks. Also, sensor networks interact closely with their physical environments and people, which will produce new security problems. Due to these constraints, it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first. [4].

Denial of service attacks on wireless sensor networks can range from simply jamming the sensor's communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or affect any other layer of the wireless sensor network. Due to the potential asymmetry in power and computational constraints, safeguarding a wireless sensor network against a well-orchestrated denial of service attack may be highly difficult. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty.

The basic requirements of WSN are

(i) Scalability- A WSN must be capable of being easily expanded or upgraded on demand.
(ii) Reliability- WSN must be worth trusting and it should provide exactly what is needed for the user.
(iii) Responsiveness- WSN should quickly react in the desired or positive way.
(iv) Mobility- WSN must be able to move from one place to another.
(v) Power efficiency- WSN must operate by spending with minimum power.

In this paper we provide a security mechanism to identify the files affected by viruses or malwares to protect the WSN.

2 Literature Survey

Chris Karlof et al. (2003) proposed security goals for routing in sensor networks, showed how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduced two classes

of novel attacks against sensor networks—sinkholes and HELLO floods, and analyzed the security of all the major sensor network routing protocols. They described crippling attacks against all of them and suggested countermeasures and design considerations. Their focus is on routing security in WSNs. According to them, the currently proposed routing protocols in WSNs optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. These routing protocols in WSNs are also insecure [1].

Al-Sakib Khan Pathan et al. (2006) analyzed the security problems in WSN and concluded that most of the attacks against security in WSN are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. At present the risk of the secure transmission of information over WSN is becoming a challenging job [2].

Yong Wang et al. (2006) analyzed the security issues in WSN and pointed that Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore an important factor in WSNs which suffers from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture and the use of insecure wireless communication channels. For a given physical access to a node in WSN, an attacker can extract sensitive information on the node. This node may also be altered or replaced to create a compromised node. So, these constraints make the security in WSNs a challenging task [3].

John Paul Walters et al. (2006) surveyed the major topics in wireless sensor network security, and presented the obstacles and the requirements in the WSN security. They also classified many of the current attacks, and finally listed their corresponding defensive measures. They also proposed that there is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature blinks a great challenge in WSN security. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource

and computing constraints, security in WSN poses different challenges than traditional network as well as computer security [4].

Eric Platon et al. (2008) proposed that in WSN cryptography constitutes the main theoretical concept, along with key infrastructures, underlying approaches that ensure integrity and confidentiality. They analyzed the general security issues of wireless sensor network research and concluded that research endeavors remain necessary, notably in dealing with the security challenges in WSN [5].

Kalpana Sharma et al. (2009) proposed an integrated comprehensive security framework in WSN that will provide security services for all services of WSN. They have simulated the above framework to test its feasibility, but the actual output will come from realistic implementation of this approach. Security concern for a WSN and level of security desired may differ according to application specific needs where the sensor networks are deployed. Improved security is especially important for the success of the WSN, because the data collected are often sensitive and the network is particularly vulnerable. While a number of approaches have been proposed to provide security solutions against various threats to the WSN, majority of them are based on the layered design and these layered approaches are often inadequate and inefficient [6].

Jaydip Sen (2009) proposed that the distributed nature of WSN and their deployment in remote areas are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is morecritical if the network is deployed for some mission-critical applications such as in a planned battlefield. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task. InWSN, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Most of thecurrent protocols assume that the sensor nodes and the base station are stationary. But practically the mobility can be at the base

station, sensor nodes, or both. Current studies on security in WSNs focus on individual topics such as key management, secure routing, secure data aggregation and intrusion detection. QoS and security services need to be evaluated together in WSNs [7].

Tahir Naeem et al. (2009) proposed a security mechanism keeping in view the architecture and limitations of WSN. They also discussed the common limitations and vulnerable features of WSN and Wireless Mesh Networks along with the associated security threats and possible countermeasures. Wireless Mesh Network is an emerging community based integrated broadband wireless network which ensures high bandwidth ubiquitous internet provision to users, but WSN is application specific and ensures large scale real-time data processing in complex environment. Both these wireless networks have some common vulnerable features which may increase the chances of different sorts of security attacks. WSN nodes have computation, memory and power limitations, which do not allow for implementation of complex security mechanism. Intrusion detection system can be a good for the multi-hop wireless networks, however, such mechanism may not be more feasible for WSN as such mechanism may increase the design complexity of sensor nodes in WSN [8].

Sona Malhotra (2011) gave brief description about the WSN security problems. Various threats due to attacks like Denial of Service (DoS), attacks during information flow, Sybil attacks, Black Hole attacks and Wormhole attacks are vulnerable in WSN. One of many security problems in WSN is absence of cryptosystem for wireless sensor networks. The cryptosystems already present are not suitable for applications in WSN. Sensor nodes are bound to the constraint on the memory and power consumption. If the encryption- decryption is implemented on the sensor nodes then the power consumption and the memory requirements are highly increased and keeping power and size constraints in mind it is not feasible [9].

Marigowda et al. (2013) provided comprehensive information on types of attacks exposed in WSN and possible methods of countering such attacks effectively. Resource constrained environment and security attacks are equally vulnerable in WSNs. When wireless sensor networks are deployed in an open or hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks [10].

Swati Bartariya et al. (2016) described some of the aspects of security like constraints, attacks, threats and security solutions in WSN after analyzing the existing WSN security approaches. According to them, WSN have recently attracted a lot of interest to the researchers due to wide range of applications. The current cryptographic mechanisms detect and defend against node compromise but there are still some compromise activities that should be detected. According to them, the deployment of new technology without security has often proved to be immoderately dangerous. Many efforts have been made on key management cryptography and defense against DoS and other attacks but still some challenges have to be addressed [11].

3 Objective:

Sensor networks are particularly affected by several types of attacks. Attacks can be performed in a variety of ways, most notably as attacks due to viruses, denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Our objective is to propose a new methodology to identify threats due to viruses and other malwares in WSN.

4 Existing Methodology

The vast majority of attacks targeting networked systems are carried out by self-replicating viruses and malwares. The available automatic tools to identify vulnerabilities and exploit them frequently scan the internet address space to find reachable targets and then try to attack them. As a consequence, a NIDS detect many attacks which cannot be effective because the targeted service may be unavailable or the exploited vulnerability may not affect any host of the controlled network. Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, etc. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Encryption mechanisms likesymmetric encryption and asymmetric encryption provides security against attacks in WSN. In symmetric encryption the receiver and the sender has to agree upon a single secret (shared) key. Decryption is the reverse of encryption, and uses the same key as in encryption. The asymmetric encryption uses public key and private key. Data encrypted by one public key can be encrypted only by its corresponding private key.

Threats affected by the nodes are malicious nodes which are responsible to trigger various attacks like wormhole attack, black hole attack, etc., in WSN. Techniques to detect and isolate malicious nodes from the network in the existing systems have to be improved. One such technique is based on the analysis of the route reply packets in which the nodes reply with the exceptional high sequence number. The nodes which send exceptional high sequence number will be considered as the malicious nodes and methods like clustering is used to isolate these nodes from the network.

In WSN the wormhole attacked malicious nodes are detected using Multi-path Hop-count Analysis (MHA) on the basis of hop-count analysis by assuming wormhole attacks have longer packet latency as compared to the normal wireless propagation latency in a single hop. As the route during wormhole seems to be shorter, various new multi-hop routes also be channeled in the direction of the wormhole that leads to the longer queuing delays. The links having delays are considered to be doubtful links, as the delay might also takes place due to congestion as well as intra-nodal processing. In this method first Hello packets has been sent to all the nodes that are within its transmission range. As soon as the receiver receives the Hello message, then it records the address of the sender and the time delay left until it will be programmed to send its next Hello message for piggybacked reply. The suspicious nodes are noted by checking the arrival time of Hello reply messages. If the arrival time is within its timeout interval then link between itself and node is taken to be safe, otherwise doubtful and communication to that node is terminated by the sender until the verification process gets over.

After this process a probing packet is sent to all the suspected nodes (that are detected in the previous step) by the sender. If a suitable acknowledgement is received from any node X within its scheduled timeout interval then node X is considered to be safe. Otherwise the occurrence of wormhole is proved. Both delay per hop indication (DelPHI) and hop count are monitored for wormhole detection. The basic assumption is that the delay that packet experience in standard conditions for propagation of one hop will become too high under wormhole.

The uniqueness of the hop-count analysis for detecting wormholes nodes is yet uncertain.

5 Proposed Methodology

The main problem in symmetric cryptography is with the keys which are used to encrypt and decrypt the data or message used to communicate the sender and receiver. The key which is used here is not more secure. In order to transfer the message in the symmetric cryptography the sender should send the key along with the message through internet in the form of e-mail or through IRC (Internet Relay Chat) services. So this type of transmission of keys is more insecure so that the data can be altered or tampered. The key can be transmitted physically but the distance between the sender and the receiver plays an important role and which is insecure. The process of transferring the key verbally through a phone line results in the leakage of the conversation to others. The sharing of the keys is also one of the problems in this type of cryptography. The other problems in this type of cryptography are key distribution and key management. This type of cryptography lacks in providing data integrity, non-repudiation and data authentication. Digital signatures cannot be created by symmetric cryptography. So, the above methods cannot rectify security threats effectively.In order to overcome the above mentioned problems a new methodology is proposed in this research to identify threats due to viruses and other malwares in WSN. Here we suggest a new approach which compares the same file at different locations and checks the basic parameters of the files using code values. Our proposed system will identify the threats due to viruses and other malwares in WSN.

6 Design and Development

The design of proposed methodology here is based on the basic file parameters. The code values of files are used to identify the presence of virus threats in the WSN. The algorithm used in the proposed system is given as follows:

Step 1: Initiate
Step 2: Input Source file.
Step 3: Calculate code values SF1 and DF1 for the file at source and destination nodes respectively.
Step 4: Compare both the code values.
Step 5: If the code values of both files match then there is no virus and other threats.
Step 6: Send the Source file to the destination node.
Step 7: Otherwise repair/delete the file at destination node.
Step 8: Request to resend the file from source node.
Step 9: Initiate virus scanning and cleaning activities at source, destination and all connected nodes.
Step 10: End.

7Experimentation and Results:

The sample experiments using the proposed method were carried out and the results were shown in the following Table 1.

File name	Code values in				Result
	Node1`	Node2	Node3	Node4	
RFID1.jpg	7BBDB4CA306F304F41E67B94693710F2	7BBDB4CA306F304F41E67B94693710F2	7BBDB4CA306F304F41E67B94693710F2	7BBDB4CA306F304F41E67B94693710F2	No Threat
scratch_sample.sb	95626538A23D1689AFB6CC9A654D9F76	95626538A23D1689AFB6CC9A654D9F76	95626538A23D1689AFB6CC9A654D9F76	74402B64C1B25F6332B851D43CFE3E92	Threats at Node4 **Virus alert and Scanning initiated at Node4**
BigData.docx	705DC976C0308B0328CFEAE880864B3A	705DC976C0308B0328CFEAE880864B3A	5DF5F0CD52E3E5967F7A059009918E98	71098E0D1EB4451C82484588AC0A952F	Threats at Node3 and Node4.**Virus alert and Scanning initiated at Nodes3 & 4**
41792.pdf	0EDAAFDFF31362AA409869A10D56FF5A	0EDAAFDFF31362AA409869A10D56FF5A	3E26884BEB0025A769FA14338F8D402D	A2A511972B15F0F0DAEBC5FC055BF386	Threats at Node3 and Node4 **Virus alert and Scanning initiated at Node3 & 4**
Natarajan1.accdb	309C87021BC5FFA4771B4C613D7DB6E0	E99298625AD04CEB334635E0B6987036	49AD594AED16823ED76A034B5E69B94B	A52BE8A534196966868D8DE81DD6D134	Threats at Node2, Node3 and Node4 **Virus alert and Scanning initiated at Node 2&3&4**

Table1: Code values in the system.

From the above table threats affected nodes are identified. Virus alert may be sent immediately and Scanning is initiated at nodes affected by threats

8 Conclusion

The WSNs continue to grow and become widely used in many applications today. However WSN suffers from many constraints like limited energy, processing capability, storage capability, as well as unreliable communications, unattended operations, etc. Providing an appropriate security method to sensor nodes is fundamental aim in WSN. Here we proposed a methodology in which the file parameters are checked at different locations using code values. In our experiments the files affected by virus threats at different nodes were identified using code values which are recorded and shown in table1. If these code values are matching then we conclude that the files are unaffected by virus like threats. We can initiate preventive actions as our proposed methodology identifies virus like threats at an earlier stage.

9 Future Work

The above proposed method is an efficient method to send and receive data and files to the desired destinations. This proposed method may be considered for further research to make improvements in the security area of WSN.

10 References

[1] Chris Karlof and David Wagner (2003), 'Secure routing in wireless sensor networks: attacks and countermeasures', Ad Hoc Networks 1 (2003) 293–315.

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hon, (2006), 'Security in Wireless Sensor Networks: Issues and Challenges', ICACT, ISBN 89-5519-129-4.

[3Yong Wang, Garhan Attebury, And Byrav Ramamurthy, (2006), 'A Survey Of Security Issues In Wireless Sensor Networks', IEEE Communications Surveys & Tutorials, www.comsoc.org/pubs/surveys.

[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, (2006), 'Wireless Sensor Network Security: A Survey', Security in Distributed, Grid, and Pervasive Computing.

[5] Eric PLATON and Yuichi SEI, (2008), 'Security software engineering in wireless sensor Networks', Special issue: The future of software engineering for security and privacy, Progress in Informatics, No. 5, pp.49–64, (2008) 49.

[6] Kalpana Sharma, M.K. Ghose and Kuldeep (2009), 'Complete Security Framework for Wireless Sensor Networks', '(IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1.

[7] Jaydip Sen, (2009), 'A Survey on Wireless Sensor Network Security', International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2.

[8] Tahir Naeem and Kok-Keong Loo,(2009), 'Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks', International Journal of Digital Content Technology and its Applications, Volume 3, No.1.

[9] Sona Malhotra (2011), 'Security Threats In Wireless Sensor Networks', Journal of Global Research in Computer Science, Volume 2, No. 5, www.jgrcs.info.

[10] Marigowda C K and Manjunath Shingadi,(2013), 'Security Vulnerability Issues In Wireless Sensor Networks: A Short Survey', International Journal of Advanced Research in Computer and Communication Engineering,Vol. 2, Issue 7, ISSN (Print) : 2319-5940
ISSN (Online): 2278-1021.

[11] Swati Bartariya and, Ashutosh Rastogi,2016, 'Security in Wireless Sensor Networks:Attacks and Solutions',International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) 2278-1021,ISSN (Print) 2319 5940,Vol. 5, Issue 3.