International Journal For Technological Research In Engineering
Volume 2, Issue 8, April-2015 *ISSN (Online): 2347 - 4718*

CENTRALIZED SIGNATURE BASED APPROACH FOR WIRELESS SENSOR NETWORK USING RSA ALGORITHM

Megha Joshi[1], Saumil Patel[2]
[1]Post Graduate Student, [2]Assistant Professor, Department of Computer Science & Engineering,
Narnarayan Shastri Institute of Technology, Jetalpur, Ahmedabad - 382426

Abstract: Recent developments in Micro-Electro-Mechanical Systems (MEMS), wireless communications, and digital electronics have enabled development of low cost, low power, multifunctional sensor nodes are small and freedom to communicate in short distances. However, it has still remained an open challenge to deploy sensor nodes in wireless environment as one has to deal with innumerable constraints for their complete implementation. In this paper, a detailed survey has been carried out related to various analysis techniques, which could be used to address present unresolved issues in wireless sensor networks.

I. INTRODUCTION

The field of sensor network is well known due to its popularity in research community. It is a collection of thousands of self-organized sensor nodes capable of wireless communication [1]. A Wireless Sensor Network (WSN) consists of sensors-equipped nodes, called motes or simply sensors, sensing the environment and reporting the collected data to one or more trusted gateway nodes, called sinks. Sinks sometimes play a coordination role, but the frequency and impact of their presence in the network is highly variable according to the setting so motes are often required to self-organize in a distributed way. WSNs are usually sensibly (sometimes even orders of magnitude) larger than similar ad-hoc networks, and are often deployed in hostile environments and over wide geographic areas [2]. WSNs can extremely be used to make easier system design and operation to monitor the environment without need connection with wired networks. Wireless sensor network is valuable technology to observe and perceive data from the physical world and has an important role in pervasive computing. However these benefits come with the several issues, vulnerability and risks. Sensor nodes have restricted in processing power, energy resource and memory. Literature review related to trust and security of WSNs is presented in different section. Structure of this paper is as follows: In section I, limitations of wireless sensor networks is discussed. In section II, security requirement is presented. Section III shows challenges of WSNs and section IV describes communication protocols for WSNs. Various attacks on WSNs and its effect is discussed in section V.

II. CONSTRAINTS IN WIRELESS SENSOR NETWORK

A great number of sensor nodes that are intrinsically resource-restricted exist in wireless sensor network. These nodes have different characteristics such as limited processing ability, so little capacity storage, and limited communication bandwidth because of restricted power and size of the sensor nodes. Sometimes it is stiff to straight use the formal security technique in WSNs. Some of the main WSN limitations include energy limitations. A WSN is susceptible to threats and risks, for example, an adversary can compromise a sensor, change the data integrity, snoop on messages, introduce wrong messages, and destroy network resource. Wireless nodes broadcast their messages to the medium differently from wired networks, so the security problems must be solved in WSNs. [3] Therefore, from above discussion, these restrictions and attaining suitable performance with security measures to address the necessities of an application are requirements in security protocols of designing need.

III. SECURITY REQUIREMENT

In making plan for secure WSNs several security services such as confidentiality, authenticity, integrity, availability must be applied.

a) Confidentiality is the ability to conceal message from the passive attacker, where the message communicated on sensor network remain confidential.

b) Integrity refers to the ability to confirm the message that has not been tampered, altered or changed while it was on the network.

c) Authentication need to know if the messages are from the node it claims to be from, determining the reliability of the message's origin.

d) Availability is to determine if a node has the ability to use the resources and the network is available for the message to move on.

IV. CHALLENGES OF WIRELESS SENSOR NETWORK

In WSN, Trust Management is difficult. Users in the wireless sensor networks are very keen to realize others' personal information, and the communication is over public accessible wireless links, so the data collection is susceptible to attacks that endanger the privacy. The communication of privacy sensitive data over civilian wireless sensor networks is regarded unpractical, without suitable protection of privacy. [3][6] In a number of mission-critical applications of Wireless Sensor Networks (WSNs), such as battlefield surveillance, disaster response, wildlife monitoring, radioactive radiation monitoring, and so on, the sensed data packets have to meet certain quality-of-service (QoS) levels in multiple domains (e.g., end-to-end delay, reliability, i.e., packet delivery ratio, network resources, and so on). For example, in radioactive radiation monitoring application, the

sensed data packets carrying radioactive leakage detection information need to be delivered to the control center within a predefined limited time while maintaining a certain level of packet delivery ratio for reliable event perception. However, due to time-varying wireless channel, dynamic network topology, and severe constraints on energy and computation power of tiny sensor nodes, achieving these QoS requirements in WSNs is a challenging problem. [4] In WSNs, constant communication infrastructure does not exist. Thus, there exist some restrictions on the communication channel between the sensor nodes which may cause problems like unreliable communication. However, it provides the broadcast advantage: A packet that has been transmitted by one sensor node to the neighboring sensor node can also be received by all the other sensor nodes deployed in WSN. Due to the large scale of WSNs, each sensor node behaves based on its local view of the entire network, including topology and resource distribution. Here, resources include battery energy and sensing, computation, and communication capabilities. To establish such a local view, techniques such as localization and time synchronization are often involved. A local view depends on the initial deployment of sensor nodes, which is itself a challenging topic. The network is usually organized using either a flat or hierarchical structure, above which topology control, MAC, and routing protocols can be applied accordingly. One key challenge is to handle network dynamics during the process of network discovery and organization. These dynamics include actuation in channel quality, failure of sensor nodes, variations in sensor node capabilities, and mobility or diffusion of the monitored entity. Autonomous adaptation of network discovery and organization protocols, in light of such dynamics, is the key to deliver proper system functionality. [5] During in-network aggregation, enemies can without difficulty change the intermediate aggregation outcomes and cause the final aggregation result deviate from the true value very much. Without security of data integrity, the data aggregation consequence is not reliable. [3]

V. COMMUNICATION PROTOCOL

a) Physical Layer: Raising the reliability by decreasing path loss impact and shadowing is the goal of physical layer. For recognized connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection, this layer is reliable.

b) Data Link Layer: Data link layer's goal is to ensure interoperability amongst communication between nodes to nodes. This layer is responsible to recognize error, multiplexing. Karlof et al suggested link layer security architecture, TinySec for WSNs to secure data link layer. For hardware based symmetric key encryption Naveen Sastry et al proposed Zigbee or the 802.15.4 standard. Moreover, to create secure key during network deployment and maintenance, some scientists suggested the probable use of public key cryptography and secure code distribution.

c) Network Layer: Providing the best path for effective routing technique is the aim of Network layer. Routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa are in charge of this layer. ID based protocols and data centric protocols are used by WSN for routing mechanism. In WSN, every node works as a router in the network (due to use broadcast method), in order to make secure routing protocol. Encryption and decryption methods are utilized for secure routing.

d) Transport Layer: For external networks i.e. sensor network connected to the internet can use Transport Layer set up communication, however it is the main difficult issue in wireless sensor networks.

e) Application Layer: Application Layer use to display ultimate yield by guarantee smooth information flow to lower layers. This layer is in charge of data collection, management and processing of the data by using the application software to obtain trustworthy consequences.

Authors provided different security protocols at different layers of wireless sensor network [6]. They described MAC and network layer protocol for use in sensor network, high level protocols for energy efficient management of sensor networks at transport layer and time synchronization and localization protocols for WSNs. Two secure and efficient data transmission (SET) protocol for CWSNs entitled SET-IBS and SET-IBOOS, by using identity based digital signature and identity based online/offline digital signature (IBOOS) scheme, respectively was proposed by authors [10]. So feasibility of proposed protocols was assessed for security requirements against various security attacks. The authors presented CENTER is a secure and efficient routing protocol that utilizes the powerful sink base station (BS) to identify and ban different types of misbehaving nodes that may interrupt or abuse the functionality of the WSN [11]. This protocol provides more efficient and secure routing while counting for the energy-constrained sensor nodes. They also presents simulation results of CENTER performed using TOSSIM to verify its correctness, security and reliability. A scheme which supports the mobility of the nodes and make the initial scheme more flexible are presented by authors [12]. The basic criterion for the evaluation of the scheme is the communication overhead and comparison with the other schemes.

VI. ATTACKS ON WSNs

In this section authors explain review about the different security attacks on the different layers briefly.

a) Denial of Service (DoS): Many kinds of DoS attacks in various layers could be presented in wireless sensor networks as an example at physical layer the DoS attacks could be jamming and tampering. At link layer, crash, and feebleness, inequitable, at network layer, neglect and greed, homing, misdirection, black holes. Jamming is a well-known attack on physical layer of wireless network. Jamming interferes with the radio frequencies being used by the nodes of a network. An attacker sequentially transmits over the wireless network refusing the underlying MAC protocol. Jamming can interrupt the network impressive if a single frequency is used throughout the network. In addition jamming can cause excessive energy consumption at a node by injecting

impertinent packets. The receiver's nodes will as well consume energy by getting those packets.

b) Wormhole attacks: A devastating attack is known as the wormhole attack, where more than two malicious colluding sensor nodes does a virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points. This tunnel establishes shorter links in the network. In which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network .Then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away [9].

C) Sinkhole attacks: The purpose of adversary in a sinkhole attack is to tempt almost all the traffic from a special network by way of a compromised node, making a metaphorical sinkhole with the adversary at the base station. Normally, by making a compromised node which appeared to be particularly interesting to encircling nodes concerning the routing algorithm, sinkhole attacks can act. Since of difficulty to confirm routing information which provided by a node, sinkhole attacks are difficult to counter. For instance, laptop-class adversary has a great power radio transmitter. This permits laptop-class adversary to supply a high-quality route by transmitting with adequate power to obtain a broad area of the network.

D) Hello flood Attack: One of the easiest attacks in WSNs is Hello flood Attack, in which attacker broadcasts HELLO packets with great transmission power to sender or receiver. The nodes receiving the messages suppose that the sender node is nearest to them and sends packets by this node. Congestion happens in the network by this attack and it is a particular kind of DOS. To prevent Hello Flood attacks, blocking methods can be used.

E) Sybil attack: The definition of the Sybil attack is a situation that a node displays higher toward identity to the networks. Fault-tolerant plans, allocate storage, and network-topology are protocols and algorithms which easily influenced. A distributed storage plan, as an example, could trust in .There being three replicas of the similar data to obtain a produced level of superfluity. When a compromised node acts as two of the three nodes, employed algorithms could deduce that redundancy being performed, in spite of the fact it has not performed. [3]

F) Selective Forwarding: A routing node has a main liability which is forwarding packets. However, any packet could be dropped and other ones might be forwarded intentionally by a malicious node. An unsuccessful detection framework to recognize the selective forwarding attack is suggested by Wang et al. The number of packets which must forward should be same to the number of packets that it receives and it is supervised for a routing node. Every sensor node can act under a promiscuous manner in their framework therefore; it can overhear the transmission of neighboring nodes. The neighbor is able to cooperate with other neighbors of the suspected node, and a decision about the suspected node is created through gathering the ideas from the suspected node's neighbors, on the condition that a neighbor of a suspected node detects exceeding a specific threshold in the packet number which failed to forward by the suspected node.[3]

VII. CONCLUSION

All of the surveyed papers focus on different methods to calculate trust and reputation and provide security for the wireless sensor network. However, it is found to utilize the centralized approach in a WSN and make use of the more powerful Base Station to perform these calculations and lessen the burden of the power consuming reputation inquiries and the computations on the sensor nodes.

REFERENCES

[1] Gaurav Sharma, Suman Balaa, Anil K. Verma, "Security Frameworks for Wireless Sensor Networks-Review" ScienceDirect, 2nd International Conference on Communication, Computing & Security [ICCCS-2012].
[2] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala," Security in Wireless Sensor Networks: Issues and Challenges", Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace)
[3] Md. Abdur Razzaque, Mohammad Helal Uddin Ahmed, Choong Seon Hong , Sungwon Lee "QoS-aware distributed adaptive cooperative routing in wireless sensor networks", (ScienceDirect) Ad Hoc Networks-2014
[4] Information processing and routing in wireless sensor networks, "Introduction to Wireless Sensor Networks", World Scientific Publishing Co. Pte. Ltd.,
[5] Junqi Duan, Yajuan Qin, Sidong Zhang, Tao Zheng, Hongke Zhang, "Issues of Trust Management for Mobile Wireless Sensor Networks" National Engineering Laboratory for Next Generation Internet Interconnection Devices, School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing,
[6] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI, "Wireless Sensor Network: Security challenges" IEEE-2012
[7] Gurudatt Kulkarni, Rupali Shelk , Kiran Gaikwad, Vikas Solanke , Sangita Gujar 5, Prasad Khatawkar, "WIRELESS SENSOR NETWORK SECURITY THREATS"
[8] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh, "Overview of Security Issues in

Wireless Sensor Networks", IEEE 2011 Third International Conference on Computational Intelligence, Modelling & Simulation.

[9] Huang Lu, Jie Li , Mohsen Guizani "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Network" (IEEE Transactions on Parallel and Distributed Systems – 2014)

[10] Ayman Tajeddine Ayman Kayssi Ali, "CENTER: A Centralized Trust-Based Efficient Routing Protocol for Wireless Sensor Networks", IEEE-2012.

[11] Saber Banihashemian · Abbas Ghaemi Bafghi · Mohammad Hossien Yaghmaee Moghaddam , "Centralized Key Management Scheme in Wireless Sensor Networks", Springer Science+Business Media, LLC. 2011

