ISSN:0975-9646

Watchdog Three-Tier Technique to Secure Wireless Sensor Network

Pramod D Mane [1], Prof. D.H.Kulkarni[2]

[1] M.E(CN) Department of Computer Engineering,SKNCOE.Pune, Maharashtra.
[2] Professors, Department of Computer Engineering, SKNCOE.Pune, Maharashtra

***Abstract*— In many wireless sensor network (WSN) the Mobile sinks(MSs) are very essential applications for efficient data gathering, restricted sensor reprogramming, and for distinguishing and revoking compromised sensors. This paper describes a Watchdog three-tier general framework that permits the use of any pairwise key predistribution scheme as its basic component. In this technique we implement a special kind of node, which is called as watchdog. This node not the part of actual communication. Watchdog checks all key of that intruder node and if key matches it allowed that node into network otherwise throwaway from the network. finally propose defending approaches that can mitigate the weaknesses of polynomial pool approach using watchdog.**

***Keywords*—Attacker, Distributed, Security, wireless sensor networks, Watchdog.**

I. INTRODUCTION

Latest advances in electronic technology have lined the way for the development of a new invention of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. [1] Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments, and habitat monitoring. The sensed data often need to be sent back to the base station for analysis. [1] [2]However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack, a sybil attack, selective forwarding ,sinkhole [1]), and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. [1] [11]

Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are critical components in the operation of many sensor network applications, including data collection in risky environments, localized reprogramming, oceanographic data collection, and military navigation. In many of these applications, sensor nodes transmit critical information over the network; [1] [11] therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data privacy and reliability a nontrivial task. [11] conventional schemes in ad hoc networks using asymmetric keys are costly due of their storage and computation cost. These limitations make key predistribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. However, the problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then start data communication with any sensor node.

To address the above-mentioned problem, we have developed a general framework that permits the use of any pairwise key predistribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and MSs. To make easy the study of a new security technique, we first refined a general three-tier security framework for authentication and pairwise key establishment, based on the polynomial pool-based key predistribution scheme. The proposed technique will significantly advance network flexibility to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach, as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework, a small fraction of the pre selected sensor nodes, called the stationary access nodes; act as authentication access points to the network, to activate the sensor nodes to transmit their aggregated data to mobile sinks. A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will begin the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink. Shown in Fig.1

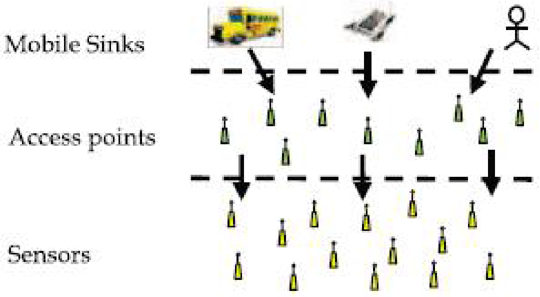

Fig1: The three-tier security scheme in WSN with mobile sinks

The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Relatively, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering.

Although the above security approach makes the network more flexible to mobile sink replication attacks compared to the single polynomial pool-based key predistribution scheme , it is still open to stationary access node replication attacks. In these types of attacks, the attacker is able to launch a replication attack similar to the mobile sink replication attack. After a portion of sensor nodes have been compromised by an attacker, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink's data request messages to activate sensor nodes to send their aggregated data. [1] [11]. Insider threat is an important security issue in wireless sensor network (WSN) because traditional security mechanisms, such as authentication and authorization, cannot catch inside attackers who are legal members of the network. Inside attackers can disrupt the network by dropping, modifying, or misrouting data packets. This is a serious threat for many applications such as military surveillance system that monitors the battlefield and other critical infrastructures. Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks [11] [12] [15]. Since WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is often implemented as a distributed system where each sensor can evaluate, update, and store the trustworthiness of other nodes based on the trust model. In general, trust mechanism works in the following three Stages 1) node behavior monitoring, 2) trust measurement, and 3) insider attack detection. Watchdog [15] is a popular monitoring mechanism for the first stage. The other two stages are processed by a trust model such as beta trust model and entropy trust model [16] using the data collected by the watchdogs. In such trust mechanism, if an inside attacker A keeps dropping packets from its neighbor N, watchdog in N will monitor and record this misbehavior by node A (stage 1). Then, node N will lower A's trust value (stage 2) and when the trust value goes below a trust threshold, N will consider node A untrusted and remove it from its neighbor list (stage 3). [18].

II Related Work

For the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then begin data communication with any sensor node. The key management problem is an active research area in wireless sensor networks. There are some earlier purposed schemes in WSN,

Eschenauer and Gilgor [3] [1] [11] proposed a probabilistic key predistribution scheme to bootstrap the initial trust between the sensor nodes. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key.

Chan et al. [4] [1] [11] further extended this idea and developed two key predistribution schemes:

- *q-composite key predistribution scheme.*
- *random pairwise keys scheme.*
- *t-degree bivariate key polynomial.*
- *q- composite key predistribution scheme:-* The qcomposite key predistribution scheme also used a key pool, but required two sensor nodes to compute a pairwise key from at least q predistributed keys that they shared.
- *random pairwise keys scheme:-* The random pairwise keys scheme randomly picked pairs of sensor nodes and assigned each pair a unique random key.
- *t-degree bivariate key polynomial:-* proposed by Liu et al. [5] [1] [11]. They developed a general framework for pairwise key establishment using the polynomial-based key predistribution protocol and the probabilistic key distribution in and. Their scheme could accept no more than t compromised nodes, where the value of t was limited by the memory available in the sensor nodes. In wireless sensor networks that make use of the existing key predistribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys.

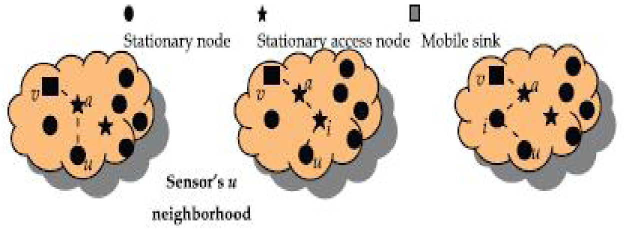

Fig 2: (a) Direct key discovery. (b) Indirect key discovery through intermediate stationary node i. (c) Indirect key discovery through intermediate stationary access node i.

In the wireless sensor networks there are major two types of attack in pairwise key establishment and authentication.

- Mobile sink replication attack.
- Stationary access nodes replication attack

A. Three-Tier Security Scheme:-

To avoid Mobile sink replication attack they used the three-tier security scheme, in this we have chosen the Blundo scheme [8] [11] to construct our approach. As we shall see, the Blundo scheme provides a clear security guarantee. Use of the Blundo scheme, therefore, greatly eases the presentation of our study and enables us to provide a clearer security analysis. In the existing scheme, they use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

Stage 1 Static and mobile polynomial predistribution:-

Stage 1 is performed before the nodes are deployed. A mobile polynomial pool M of size mod M and a static polynomial pool S of size mod S are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given Km and one polynomial (Km >1)from M. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node. This assures that a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of Km and Ks-1 polynomials from S. Fig. 2 shows the key discovery between the mobile node and stationary node.

Stage 2 Key discovery between mobile node and stationary node:-

To establish a direct pairwise key between sensor node u and mobile sink v, a sensor node u needs to find a stationary access node a in its neighborhood, such that, node a can establish pairwise keys with both mobile sink v and sensor node u. In other words, a stationary access node needs to establish pairwise keys with both the mobile sink and the sensor node. It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. To discover a common mobile/static polynomial, a sensor node i may broadcast a list of polynomial IDs, or alternatively, an encryption list

$$E_{kv}(\alpha)_{,v = 1\ldots,\mathrm{mod}}\, K_{si} \qquad \ldots\ldots\ldots\ldots\ldots\ (1)$$

where Kv is a potential pairwise key and the other node may have as suggested in [3]and [4]. When a direct secure path is established between nodes u and v, mobile.

B. The Enhanced Three-Tier Security Scheme:-

To avoid stationary access node replication attack they used the three-tier security scheme, As described above, the three-tier security scheme provides better network resilience against mobile sink replication attack compared to the single polynomial pool approach. This scheme delivers the same security performance as the single polynomial pool approach when the network is under a stationary access node replication attack.

C. Watchdog:-

Marti et al [15] introduced a monitoring mechanism known as watchdog to identify misbehaving nodes in wireless ad hoc networks. In their approach, each sensor node has its own watchdog that monitors and records its one hop neighbors' behaviors such as packet transmission. When a sending node S sends a packet to its neighbor node T, the watchdog in S verifies whether T forwards the packet toward the BS or not by using the sensor's overhearing ability within its transceiver range. In this mechanism, S stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match. If yes, it means that the packet is forwarded by T and S will remove the packet from the buffer. If a packet remains in the buffer for a period longer than a pre-determined time, the watchdog considers that T fails to forward the packet and will increase its failure tally for T. If a neighbor's failure tally exceeds a certain threshold, it will be considered as a misbehaving node by S. Watchdog works similarly with trust mechanism in that trust model evaluates each sensor's trustworthiness based on the past behaviors in much sophisticated ways. In this paper, to avoid any confusion, we consider that watchdog is a component in the trust mechanism and it is responsible for node behavior monitoring. [18]

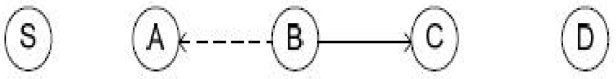

Fig 3: Example of Watchdog.

Watchdog [15] is a representative agent, which is used to monitor packet transmission to neighbouring nodes in an ad hoc network. Watchdog saves packets using a Watchdog monitoring buffer before packet transmission in order to monitor packets relaying from a neighbouring node to the next node. [17]

Fig 3 shows an example of watchdog. 'S' is the sender node and 'D' is the destination node (base station), while the other nodes are intermediate nodes in the route. When node 'A' receives a packet from his neighbouring node sender 'A', 'A' relays the packet to its neighbour on the route to the destination. Before transmission, the Watchdog agent module of node 'A' saves the packet on its Watchdog monitoring buffer. After packet transmission to node 'B', 'A' waits to check that the packet relays from its neighbouring node 'B' to the next node 'C' on the route. When node 'B' retransmits the packet received from node 'A' to the next node 'C', node 'A' also receives the packet because ’A’ is also within the transmission range of node ’B’.

Thus, node ’A’ compares the packet received from node ’B’ with that saved by the Watchdog monitoring buffer. If the packet is not the same or if it is not transmitted within the time period defined by node ’B’, the Watchdog on node ’A’changes the confidence level of node ’B’. [17]

III PROPOSED SYSTEM

In Existing method intruder is allowed to move easily inside network, so there is a threat that it may cause physically or congestion to other node. To avoid this, we implement a special kind of node, which is called as watchdog. This node does not involve in communication, if attacker is detected by access point, access point will send message to watchdog, then watchdog check the keys, if key matches then permit that node into network otherwise it will throw that node out of the network.

IV CONCLUSION

An attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. To avoid this we proposed a watchdog three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme and watchdog node, substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach. [1]

REFERENCES

[1] Amar Rasheed, Student Member, IEEE, and Rabi N.Mahapatra, Senior Member, IEEE ”The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks,” IEEE Transactions on Parallel And Distributed Systems, vol. 23, no. 5, May 2012.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,”Wireless Sensor Networks: A Survey,”Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[3] L. Eschenauer and V.D. Gligor, ”A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security CCS ’02, pp. 41-47, 2002.

[4] H. Chan, A. Perrig, and D. Song, ”Random Key Pre- Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[5] D. Liu, P. Ning, and R.Li. Establishing, ”Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS’03), pp. 52-61, Oct. 2003.

[6] A. Rasheed and R. Mahapatra, ”A Key Pre- Distribution Scheme for Heterogeneous Sensor Networks,”Proc. Int’l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC ’09), pp. 263-268,June 2009.

[7] L. Lamport, ”Password Authentication with Insecure Communication,”Comm. ACM, vol, 24, no. 11, pp.770-772, Nov. 1981.

[8] C.Blundo, A.De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ”Perfectly-Secure Key Distribution for Dynamic Conferences,” Proc. 12th Ann. Int’l Cryptology Conf. Advances in Cryptology(CRYPTO ’92), pp. 471-486, 1993.

[9] R.Viswanathan, J.Vignesh Kumar, T.V.Krishna Prasad, ”Analyzed Virtual Routing Protocol for FutureNetworks (MANET and topological network)”International Journal of Distributed and Parallel Systems(IJDPS) Vol.3, No.4, July 2012.

[10] Rasheed and R.Mahapatra,”An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks,”Proc.IEEE 27th Int’l Performance Computing and Comm.Conf. (IPCCC ’08), pp.264-270,Dec.2008.

[11] D.David Neels Pon Kumar,K.Arun Kumar, M.S.Arthy, ”An Overview of Mobile Sink and Static Access Node Replication Attacks in WSN”,International Journal of Engineering Science and InnovativeTechnology(IJESIT),Volume1,Issue2,November 2012,pp.313-320.

[12] Denis Tr ek,”Trust management in the pervasive computing era,”IEEE Security and Privacy,Vol.9,No.4,July 2011, pp.52-55.

[13] Vijay Varadharajan, ”A Note on Trust-Enhanced Security”, IEEE Security and Privacy, Vol. 7, Issue 3, May 2009, pp. 57-59.

[14] Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, ”Trust mechanisms in wireless sensor networks: attack analysis and countermeasures,” Journal of Network and Computer Applications, Elsevier, 2011, in press.

[15] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, ”Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks,” In Proc. Of International Conference on Mobile Computing and Networking (Mobicom), 2000, pp. 255-265.

[16] Yan (Lindsay) Sun, Zhu Han, and K. J. Ray Liu, ”Defense of Trust Management Vulnerabilities in Distributed Networks,” IEEE Communications Magazine, Vol 46, Issue 2, 2008, pp.112-119.

[17] Jongbin Ko, Jungtaek Seo, Eui-Jik Kim and Taeshik Shon, ”Monitoring Agent for Detecting Malicious Packet Drops for Wireless Sensor Networks in the Microgrid and Grid-enabled Vehicles” nt J Adv Robotic Sy, 2012, Vol. 9, 31:2012.

[18] Youngho Cho and Gang Qu Yuanming Wu, ”Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks”, IEEE CS Security and Privacy Privacy Workshops,2012,pp.134-141.