ISSN Online: 2319 – 9253
Print: 2319 – 9245

AN EFFICIENT SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS WITH MOBILE SINKS

#1AMOL ABHIMAN MAGAR, Pursuing M.Tech,
#2B.S.SONAWANE, ***Asst. Professor,***
Dept of CSE
MIT COLLEGE, AURANGABAD (MS), INDIA.

Abstract: Wireless sensor networks consisting of a large number of low power, low cost sensor node that communicate wirelessly. Such sensor networks can be used in wide range of applications such as military sensing and tracking, health monitoring etc, when the sensing field is too far from the station, transmitting data over long distance using multi-hop may weaken the security strength. To overcome this problem, mobile sinks (MS) are used. Mobile sinks plays a vital role in many wireless sensor applications for efficient data collection and localized sensor reprogramming. MS prolong the lifetime of the sensor network. Security became a critical issue when sensor network with MS are deployed in hostile environment. For providing more security against clone attack and Sybil attack, the proposed scheme implements mobile sink server to offer better security. In Sybil attack, the malicious device illegitimately taking on multiple identities whereas in, clone attack, adversaries may easily capture and compromise sensors and deploy unlimited number of clones of the compromised nodes. Based on the parameters such as bandwidth utilization, speed and time, the malicious act by the adversary are detected. And MS is assigned randomly once it is exposed to threat. In the traditional schemes an attacker can easily obtain large number of keys by capturing small fraction of nodes and initiate data communication with any sensor node. Here the main focus is on the sensor network that uses mobile sink to gather the sensed data from the network. A new security technique- Three tier security scheme is proposed to provide authentication and pair wise key establishment between sensor nodes and mobile sinks. The proposed scheme makes use of two polynomials pools: static polynomial pool and mobile polynomial pool which will improve network resilience to the mobile sink replication attack.

Keywords: Distributed. Security, Wireless Sensor networks, AODV, Mobile Sink.

I.INTRODUCTION

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. Some of the popular applications of sensor network are area monitoring, environment monitoring (such as pollution monitoring), industrial and machine health monitoring, waste water monitoring and military surveillance.

In Mobile Sink Wireless Sensor Networks (MSWSN), all sensors are static other than the sink node. Mobile nodes are the destination of messages originated by sensors, i.e., they represent the endpoints of data collection in the network. They can either autonomously consume collected data for their own purposes or make them available to remote users by using a long range wireless Internet connection. In sensor nodes are static and densely deployed in the sensing area. One or multiple Mobile sinks (MS) move throughout the network to collect data from all sensors. Communication between the source sensors and the MS is either single hop or multi-hop.

During the data collection technique in mobile sink sensor networks, security is an important factor. Node need to be authenticate before start the data collection process. At the same time sensors also need to authenticate the sink. After authentication takes place the start the data communication process with specified rule. During the data collection sensor send their data with encrypting the data packets and send it to the sink node. When sink receive the data it decrypt the packet and check for the adversary modification during data transmission. This node authentication, data encryption and decryption use different cryptography technology. Using cryptography function it secures the communication process.

Mobility is exploited in the field of wireless sensor network to circumvent multi-hop relaying and to reduce energy consumption at nodes near the base station, and hence elongate the lifetime of the network. Mobile elements already exist in the deployment environment; a network node can be attached to these mobile elements for data collection.

Here we focus on a sensor network that uses mobile sink to gather sensor data. Security is a critical issue when sensor networks are deployed in hostile environment where they are exposed to a variety of malicious attacks. For eg., an adversary can easily monitor the traffic, capture sensor nodes, impersonate a mobiles sink to gather sensor data and provide misleading information. In many of these applications, sensor nodes transmit critical information over the network. Therefore security services such as authentication and pair-wise key establishment between sensor nodes and mobile sinks are important. However the resources constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a non-trivial task. To overcome the sink and nodes replication attacks, a three tier security scheme is developed that make use of any pair-wise key pre-distribution scheme as its basic component, to provide authentication and pair-wise key establishment between sensor nodes and mobile sinks. This technique will improve the network security to mobile sink replication attacks compared to the previous schemes where an attacker has to compromise many sensor nodes in the network to achieve a successful mobile sink replication attack. Although the above security approach makes the network more resilient to mobile sink replication attack, it is still vulnerable to stationary access node replication attack. To make three tier security scheme more effective against a stationary access node replication attack, we have strengthened authentication mechanism between stationary access nodes and sensor nodes using one way hash algorithm in conjunction with static polynomial pool based scheme.

Mobile Sink Wireless Sensor Network:

In Mobile Sink Wireless Sensor Networks all the sensors are statically deployed to sense the environment and mobile sink traverse the networks. It overcomes the problem of the sink neighborhood problem. In the sink neighborhood problem is neighbor nodes of sink participate more in the data transmission. The result is the faster energy deplete compared to other nodes in the network. If we look over the energy conservation model sensor deplete some amount of energy during the data receiving and the data transmission. As the sensor those are close to the sink, participate more data transmission i.e. for them and for those sensors away from the sink in the same direction.

A malicious node can participate in the data collection process by showing it as the sink node. Then all the sensed data collected by the malicious node, for that we need to authenticate the node before sending the sensed data. If sensors send its packets without encryption then malicious node can accept the packet then it can modify the content of the packet. So we'll lose the original content of the data. Data is neither to be modified nor be dropped. We need to keep data freshness. Otherwise, mobile elements are part of the network infrastructure itself and can be controlled by the network. There exist a number of sensor networks applications that use mobile sinks in their operations, such as data collections in hazardous environments, localize reprogramming, and military navigation. Due to the their operating nature, they often left unattended, hence prone to different kinds of malicious attacks such as the Sybil attacks, clone attacks and wormhole attacks.

II.SYSTEM DESCRIPTION AND PROBLEM STATEMENT

Wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. 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. However, when the sensing field is too far from the base station, transmitting the data over long distances using multi-hop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a clone attack, a sybil attack, selective forwarding, sinkhole, and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor network applications, including data collection in hazardous environments, localized reprogramming, oceanographic data collection, and military navigation. For the basic probabilistic [17] and q-composite [18] 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 initiate data communication with any sensor node

2.1. Existing Work:

In the existing system, the security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution scheme, it is still vulnerable 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 fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink's data request messages to trigger sensor nodes to send their aggregated data. It use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial [19] 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. Hence it overcomes mobile sink replication attack [16] and stationary access node replication attack. But it doesn't overcomes clone attack and Sybil attack.

2.2. Proposed System:

In the proposed system, Mobile sink servers are implemented to mitigate and over Sybil and clone attack. MS collects data from the sensor node and it is forwarded to MSS and hence to the base station. MSS monitors MS based on parameters such as time, delay and traffic. It act as a guard node incase of Sybil attack and witness node in clone attack. As a guard node it will monitor the traffic and misbehave MS node and sends alert to sensor node, not to forward the sensed data. Thus the mobile sink is revoked from the network and MS is assigned randomly. Clone attack uses RED(Randomized Efficient and Distributed) protocol, witness node will check for the random number, node ID and location ID which is generated with the user information. This system uses AODV routing protocol.

2.3. SYBIL ATTACK:

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities.

2.4. CLONE ATTACK:

Adversaries may easily capture and compromise sensors and deploy unlimited number of clones of the compromised nodes. Since these clones have legitimate access to the network (legitimate IDs, keys, other security credentials, etc.), they can participate in the network operations in the same way as a legitimate node, and thus launch a large variety of insider attacks or even take over the network. If these clones are left undetected, the network is unshielded to attackers and thus extremely vulnerable. Most existing research efforts in sensor networks against clone attacks focus on preventive technologies rather than detective techniques, e.g., key schemes to prevent sensors from being compromised. Unfortunately, most of these preventive technologies (i.e., key schemes) may easily lose their power against clone attacks [11]. Therefore it is imperative to provide effective/efficient clone attack detection.

2.5. AODV:

AODV [8] is an on-demand, single path, loop-free distance vector protocol. It combines the on-demand route discovery mechanism in DSR with the concept of destination sequence numbers from DSDV. However, unlike DSR which uses source routing, AODV takes a hop-by-hop routing approach.

2.5.1. ROUTE DISCOVERY AND ROUTE MAINTENANCE:

2.5.1.1. ROUTE DISCOVERY:

In on-demand protocols, route discovery procedure is used by nodes to obtain routes on an ‘as needed’ basis. In AODV, route discovery works as follows. Whenever a traffic source needs a route to a destination, it initiates a route discovery by flooding a route request (RREQ) for the destination in the network and then waits for a route reply (RREP). When an intermediate node receives the first copy of a RREQ packet, it sets up a reverse path to the source using the previous hop of the RREQ as the next hop on the reverse path. In addition, if there is a valid route available for the destination, it unicasts a RREP back to the source via the reverse path; otherwise, it re-broadcasts the RREQ packet. Duplicate copies of the RREQ are immediately discarded upon reception at every node. The destination on receiving the first copy of a RREQ packet forms a reverse path in the same way as the intermediate nodes; it also unicasts a RREP back to the source along the reverse path. As the RREP proceeds towards the source, it establishes a forward path to the destination at each hop.

2.5.1.2. ROUTE MAINTENANCE:

Route maintenance is done by means of route error (RERR) packets. When an intermediate node detects link failure (via a link-layer feedback, e.g.), it generates a RERR packet. The RERR propagates towards all traffic sources having a route via the failed link, and erases all broken routes on the way. A source upon receiving the RERR initiates a new route discovery if it still needs the route. Apart from this route maintenance mechanism, AODV also has a timer-based mechanism to purge stale routes.

In the basic probabilistic and q-composite key pre-distribution schemes, an attacker can easily obtain large number of keys by capturing a small fraction of network sensor nodes, making it possible for the attacker to take control of the entire network by deploying replicated mobiles sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node. Traditional schemes in ad-hoc networks using asymmetric keys are expensive due to their storage and computation cost. These limitations make key pre-distribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. In basic probabilistic key distribution each sensor node randomly picks a set of keys from the key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key. The q-composite key pre distribution scheme is based on the basic probabilistic scheme but it requires two sensors to share at least q-pre distributed keys to establish a pair wise key.

III. IMPLEMENTATION METHODS

A general framework is developed in order to provide authentication and pair-wise key establishment, based on polynomial pool based key pre-distribution scheme. The proposed technique will improve network resilience to mobile sink replication attacks as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool and hence more security is provided than previous approaches. 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 initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink.

A. PROPOSED SYSTEM ARCHITECTURE

Fig. 1 represents the overall flow of the project. The stationary access nodes shown above act as authentication access points to the network to trigger the sensor nodes to transmit their aggregated data to the mobile sinks. A mobile sink sends data request message to the sensor nodes via stationary access nodes. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to requested mobile sink. The proposed scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from mobile polynomial pool are used to establish authentication between mobile sinks and stationary access nodes which enable mobile sinks to access the network for data gathering. Polynomial from static pool is used to establish authentication and key setup between sensor nodes and stationary access nodes.

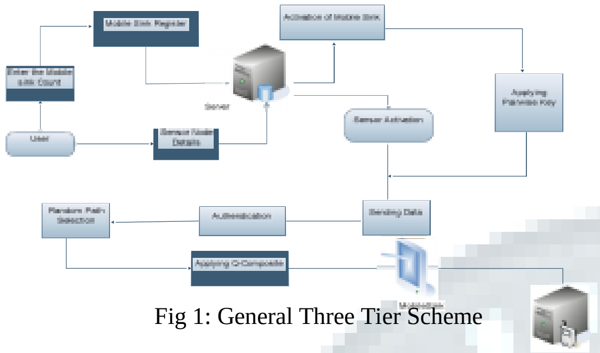

Fig 1: General Three Tier Scheme

B. SENSOR NODE DEPLOYMENT

In this module, we create many sensor nodes. Users enter the sensor name, IP address, port number and status of the node to register in the database. While entering the next node user has to check in the database where that node already exists in the database. Later for activation of sensor nodes the user should enter the details of the particular sensor node which he wants to activate and click on the activate icon that appears in the dialogue box and the nodes get successfully activated.

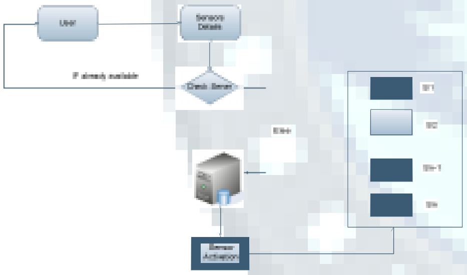

Fig 2: Sensor node deployment

C. CREATING MOBILE SINKS

In this module, we create mobile sink. User should enter the number of mobile sinks he wants to create, mobile sink name, I P Address, port number, status of the mobile sink to register in the Database. While entering the next mobile sink user has to check in the database where that particular mobile sink already exists in the database. Later for successful activation of mobile sink, user shuld enter the details of the mobile and click on the activate icon.

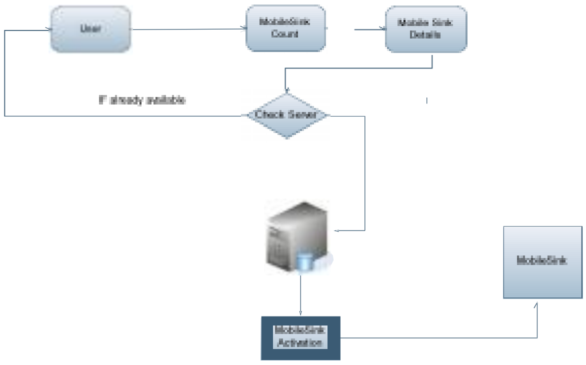

Fig 3: Creating mobile sinks

D.AUTHENTICATION & PAIR WISE KEY DISTRIBUTION

In this module, we are going to authenticate all the sensor node and mobile sink and these authenticated mobile sinks are managed by polynomial pool both static as well as dynamic. 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. Rather, 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.

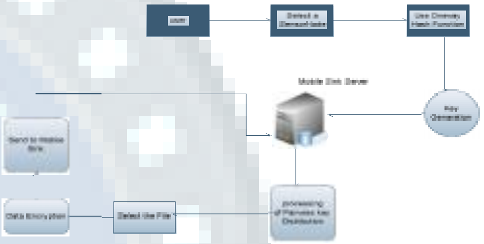

Fig 4: Pair wise key distribution scheme

IV.PERFORMANCE METRICS

4.1. Throughput/ Delivery Ratio

In Wireless Sensor Networks throughput is the average rate of successful message delivery over communication radio. This data may be delivered by the physical or logical link, or pass through certain network nodes. The throughput is usually calculated in bits per second (bps), and sometimes in data packets per second or data packets per time slot. Yuxi et al. [12] showed that lossy links do have significant impact on the maximum achievable throughput. There are some cases, where a network can achieve half of the throughput of the corresponding lossless network. Lossy links also affects energy efficiency. Lossy network can only achieve half of the throughput when links are lossless.

4.2. Network Life Time

Network lifetime is the key characteristic for evaluating sensor networks in an application specific way. The lifetime of sensor network depends on the operation time of individual sensor nodes. Lifetime of wireless sensor networks ends when first node dies in the network. Y. Chen et al. [7] described two key parameters at the physical layer that affect the lifetime of the network: the state of the channel and the residual energy of sensors. Here in this letter they proposed a greedy approach to lifetime maximization which achieves considerable improvement in the lifetime performance.

4.3. Data Freshness

In [14] Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh.

Informally, data freshness denotes that the data is recent, and it confirms that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request response pair, and allows for delay estimation [14]. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network [15].

VI.CONCLUSION

The proposed scheme based on polynomial pool based pre distribution scheme substantially improves network resilience to mobile sink replication attack compared to single polynomial pool based pre distribution approach. Analysis indicates that with 10 percent of sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach. The proposed scheme is based on mobile sink server which determines the parameters such as traffic, time and bandwidth of all the mobile sink. An uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. If the node misbehaves it revokes and assign MS randomly. Thus the replication of node and its identity can be resolved. Hence data collection can be done in secure manner. All the simulation has been carried out with NS 2.34. This thesis is supported by the literature survey in the area of Mobile Sink Wireless Sensor Networks to make it complete.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” The International Journal of Computer and Telecommunications Networking Computer Networks, vol. 38, no. 4, pp. 393-422, March 2002.

[2] I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, “Sink mobility protocol for data collection in wireless sensor networks,” Proc. of the 4th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC’06), pp. 52-59, 2006.

[3] S. Basagni, A. Carosi, E. Melachrinoudis, C. Petrioli, and Z. M. Wang, “Protocols and model for sink mobility in wireless sensor networks,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 10, no. 4, pp. 28-30, 2006..

[4] L. Cheng, Y. Chen, C. Chen, and J. Ma, “Query-based data collection in wireless sensor networks with mobile sinks,” Proc. of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, pp. 1157-1162, 2009.

[5] B. Parno, A. Perrig, and V. D. Gligor, “Distributed detection of node replication attacks in sensor networks,” Proc. of the 2005 IEEE Symposium on Security and Privacy (S&P’05), pp. 49–63, 2005.

[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key pre-distribution scheme for wireless sensor networks,” In ACM CCS 2003, pages 42{51,Oct. 2003}.

[7] Yunxia Chen and Qing Zhao ”On the Lifetime of Wireless Sensor Networks,” IEEE communications letters, vol. 9, no. 11, pp. 976-978, November 2005.

[8] Charles E. Perkins and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector Routing,” Proceeding of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), New Orleans, LA, USA, February 1999, pages 90-100.

[9] Murat Demirbas and Youngwhan song, “An RSSI-based Scheme for Sybil Attack Detectionin Wireless Sensor Networks,”Proceeding of the 2006 International symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM’06), pages 564- 570.

[10] Kai Xing, Fang Liu, Xiuzhen Cheng, David H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," icdcs, pp.3-10, 2008 The 28th International Conference on Distributed Computing Systems, 2008.

[11] H. Choi, S. Zhu, and T. Laporta. Set: Detecting node clones in sensor networks. In SecureComm’07, 2007.

[12] Li, Harnes, Holte, ”Impact of Lossy Links on Performance of Multihop Wireless Networks,” IEEE, Proceedings of the 14th International Conference on Computer Communications and Networks, pp. 303 - 308, Oct 2005.

[13] Amar Rasheed and Rabi N. Mahapatra, “The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks,” Proceedings of the IEEE Transactions on parallel and distributed systems, VOL. 23, NO. 5, MAY 2012.

[14] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J. D. Tygar, ”SPINS: Security Protocols for Sensor Networks,” Wireless Networks, pp. 189-199, 2001.

[15] Apostolos, Pyrgelis. ”Cryptography and Security in Wireless Sensor Networks,” Department of Computer Engineering and Informatics, 2009.

[16] J. R. Douceur, “The Sybil attack,” In First International Workshop on Peer-to-Peer Systems (IPTPS '02), Mar. 2002.

[17] 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.

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

[19] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, “Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors,” Proc. 13th Int’l Conf. Computer Comm. and Networks (ICCCN ’04), Oct.2004.