ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Intrusion Resilience Using Self-Healing Mechanism in Mobile Unattended WSNs

Yuvapiriyaa T[#1], Pradeepa R[*2]

[#]Department of Computer Science and Engineering, M.Kumarasamy College Of Engineering, Karur, India .

M.Kumarasamy College Of Engineering, Karur, India

Abstract— Wireless Sensor Networks (WSNs) has an immediate change to a wide range of attacks due to some distributed nature, limited sensor resources, and lack of tamper resistance. Once a sensor is corrupted, the adversary learns all secrets. Hence, most of the security measures become ineffective. Recovering secrecy after compromise requires either help from a trusted third party or access to a source of high-quality cryptographic randomness. Neither is available in Unattended Wireless Sensor Networks (UWSNs), often the sink visits the nodes. In previous results it has been shown that the sensor collaboration is an effective but expensive means of obtaining probabilistic intrusion resilience in static UWSNs. Hence it focus on intrusion resilience in Mobile Unattended Wireless Sensor Networks, where sensors move according to some mobility models. Such that a mobility feature could be independent from security (e.g., sensors move to improve area coverage). It defines a security metrics to evaluate intrusion resilience protocols for sensor networks. The proposed system uses cooperative protocol that by leveraging sensor mobility which allows compromised sensors to recover secure state after compromise. Hence it is obtained with very low overhead and in a fully distributed fashion.

Keywords— WSN security, intrusion resilience, distributed adversary, self-healing, mobility.

I. INTRODUCTION

A Wireless Sensor Network (**WSN**) in its simplest form can be defined as a network of possible devices denoted as nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links, the data is forwarded, possibly via multiple hops relaying, to a sink that can use it locally, or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. It can be homogeneous or not.

Sensor networks, which are composed of a number of sensor nodes with limited resources, have been demonstrated to be useful in applications such as home, environmental, industrial.

The sensor network consists of sensor nodes with IDs. The communication is assumed to be symmetric. In addition, each node is assumed to periodically broadcast a beacon containing its ID to its neighbors. This is usually

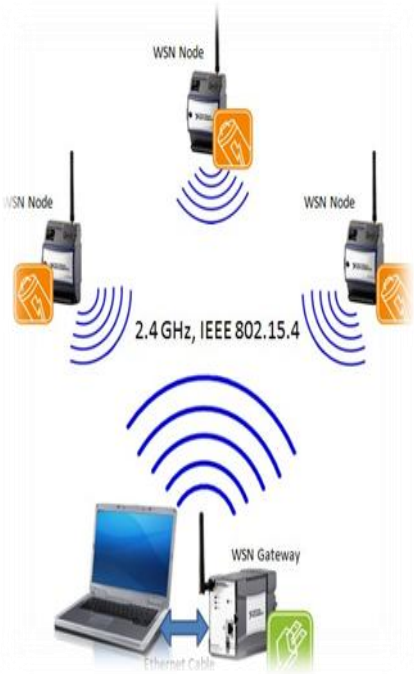

Fig 1.2 Wireless Sensor Networks

required in various applications, for example, tracking. The time is divided into time intervals, each of which has the same length. The sensor nodes have mobility and move according to the Random Way Point (RWP) model which is commonly used in modelling the mobility of *adhoc* and sensor networks. Each node is assumed to be able to be aware of its geographic position. Each node randomly chooses a destination point (waypoint) in the sensing field, and moves toward it with velocity, randomly selected from a predefined interval.

A. Unique characteristics of WSNs

1) *Communication paradigm:* Compared to traditional communication networks, individual node Identifiers (IDs) are not important. Instead, WSNs are data centric meaning that the communication should be targeted to nodes in a given location or with a defined data content.

2) *Application specific:* WSN is deployed to perform a specific task.

3) *Dynamic nature:* In a typical WSNs, node platforms are error-prone due to harsh operating conditions. Communication links between nodes are not stable due to node errors, unreliable and simple modulations, mobility of nodes, and environmental interferences.

4) *Scale and density:* Compared to other wireless networks, the number of nodes comprising WSNs may be huge. Further, the density of nodes can be high.

5) *Resource constraints :* A typical WSN node is small in physical size and battery powered. This implies that computation, communication, and memory resources in nodes are very limited.

6) *Deployment :*In large-scale WSNs, the deployment of nodes is random and their maintenance and replacement is impractical. Still, the requirements and applications of the deployed WSN may alter, which implicate that runtime reconfiguration and reprogramming are needed.

7) *Fault tolerance:* The network functionality must be maintained even though the built-in dynamic nature and failures of nodes due to harsh environment, depletion of batteries, or external interference make networks prone to errors.

8) *Lifetime:* The nodes are battery powered or the energy is scavenged from the environment and their maintenance is difficult.

9) *Scalability:* The number of nodes in WSN is typically high. Thus, the WSN protocols must deal with high densities and numbers of nodes.

10) *Realtime:* WSNs are tightly related to the real world. Therefore, strict timing constraints for sensing, processing, and communication are present in WSNs.

11) *Security:* The need for security in WSNs is evident, especially in health care, security, and military applications. Most of the applications relay data that contain private or confidential information.

12) *Production cost:* The number of nodes in WSNs is high, and once nodes run out of batteries they are replaced by new ones. Further, WSNs are envisioned to be everywhere. Therefore, to make the deployments possible, the nodes should be extremely low cost.

B. Unattended Wireless Sensor Networks(UWSNs)

In UWSN Mobile Adversary (ADV) defined by:

Goal :	Search-and-erase
	Search-and-replace
	Curious
Operation :	Reactive
	Proactive
Visibility:	Stealthy
	Visible

II. Related Work

The sensors can recover the lost session keys on their own Dutta et al. [11] proposed a constant storage self-healing protocol for WSNs. Sensor key update uses a polynomial-based secret sharing scheme, performed with the help of the sink. The sink periodically broadcasts information to allow non revoked sensors to update their current session key. At any time, sensors can be revoked and prevented from learning keys of any sessions after revocation. Hence, it is achieved by self-healing key distribution scheme.

If the Sensor node has been compromised, the security of the network degrades quickly[12].Anomaly-based intrusion detection system is used to detect those compromised nodes.

In the unattended setting, a sensor is unable to communicate to a sink at all time DISH (Distributed Self-Healing) scheme[13]used to maintain secrecy of collected data by each sensor.

Unattended sensors can not immediately overload data to a safe external entity (such as a sink).The adversary can erase or modify target data. Maximising the chances of data survival[14].

WHISPER[15] provides both backward and forward secrecy for keys shared between any two sensors. Session keys are computed from two secrets, provided by each party.

III. Adversarial Model

It provides details with the adversarial model. Hence this techniques can be applied to UWSN deployed on any fixed-area surface: Uniform coverage only helps our analysis.

Mobility: Sensor sj starts at position and moves over the deployment area according to a network-wide mobility model. Mobility Sensor sj starts at position and

moves over the deployment area according to a network-wide mobility model.

Let us consider two mobility models:

- *Random Jump Mobility Model (RJ)*: Each sensor sets its speed so it can reach any point of the sphere in one round. Starting with round r ¼ 1 and initial position, sj chooses a random point and moves there atomically.
- *Random Waypoint Mobility Model (RP):* All sensors move with the same constant speed and can cover at most distance m in a single round.

Based on sensor compromise and the adversary knowledge of its secrets, the set of sensors can be partitioned into three distinct groups at any round:

- *Red sensors (Rr):* A sensor sj is red if it is currently compromised and its secrets are exposed to the adversary.
- *Yellow sensors (Yr):* A sensor sj is yellow if it is not currently compromised but ADV still knows its secrets for the current round.
- *Green sensors (Gr*): A sensor is green if its current secrets are unknown to ADV. This is because either it has never been compromised or because it has recovered secrecy via the key-insulated protocol.

Main goals of the adversary are:

- Either to minimize the number of green sensors, or to keep a specific sensor compromised for as long as possible.
- To assess the effectiveness of a generic key-insulated protocols we define two new metrics:
  Health Ratio (HR) and
  Healthy Cycle (HC).

IV. Collaborative Intrusion Resilience Protocol

Algorithm:
Collaborative Intrusion-Resilient Protocol.
Move();
d^r_j= Read();
K^r_j=PadGen(K^r_j);
Store(E_{PK}(K^r_j, d^r_j,r,s_j));
R^r_j=[];
c = 0;
t = RandGen(K^r_j);
Broadcast(t);
while (roundTimer) do
Receive t^r_p from s_p;
R^r_j[c]= t^r_p;
C=c+1;
end

In collaborative intrusion resilience protocol in Mobile UWSNs(UWSNs) has been introduced where unattended sensors migrate within a fixed deployment area and gather environmental data waiting for the sink to approach the network and to collect them.

The main goal is to design techniques that enable sensors to recover secrecy of their cryptographic material (e.g., keys) after compromise. Thus the impact on collaborative intrusion resilience of sensor mobility models and number of regions controlled by the adversary.

ADV's location is unknown and sensors cannot distinguish between compromised and non compromised peers, the protocol is proactively run by all sensors.

To reach this goal, there are two general metrics to assess the effectiveness of intrusion-resilient protocols for UWSNs and later propose a collaborative distributed protocol that leverages sensor cooperation and locomotion to achieve probabilistic key insulation.

Sensors take advantage of mobility and collaboration with peers to regain secrecy after having been compromised by inadvertently wandering into the area under adversarial control.

In collaborative intrusion resilience protocol, forward secrecy is (predictably) obtained with periodic secret evolution using PRNG. The main idea is for sensors to serve as a source of randomness for their peers in order to obtain backward secrecy.

A sensor that resides outside the area controlled by ADV, but whose secrets are exposed (that is, a yellow sensor), can regain security and move to a new secure state (i.e., become green) if it obtains at least one contribution of secure randomness from a peer sensor whose secret state is not exposed (green sensor).

As the adversary eavesdrops on red sensors, their received contributions are observable, so they cannot regain secrecy. Our protocol leverages mobility to bring computationally secure randomness to yellow sensors. Since ADV's location is unknown and sensors cannot distinguish between compromised and non compromised peers, the protocol is proactively run by all sensors.

IV. Proposed Model

In proposed system, to simplify the analysis, at each round, the sensors are partitioned into three distinct groups. Sensors move, the network can guarantee optimal area coverage, even if precise sensor deployment is infeasible (e.g., because of hostile or inaccessible conditions of the deployment area). Moreover, mobile sensors can extend sensor lifetimes bringing energy to sensors with depleted batteries.

Based on sensor compromise and the adversary knowledge of its secrets, the set of sensors can be partitioned into three distinct groups at any round:

A sensor can be red, yellow, or green, as defined next:

- A green sensor remains green until it moves at distance less from ADV.
- A red sensors cannot become green without becoming yellow first as ADV eavesdrops on red sensors.

- A yellow sensors can become green only if it receives at least one contribution from a green sensor.

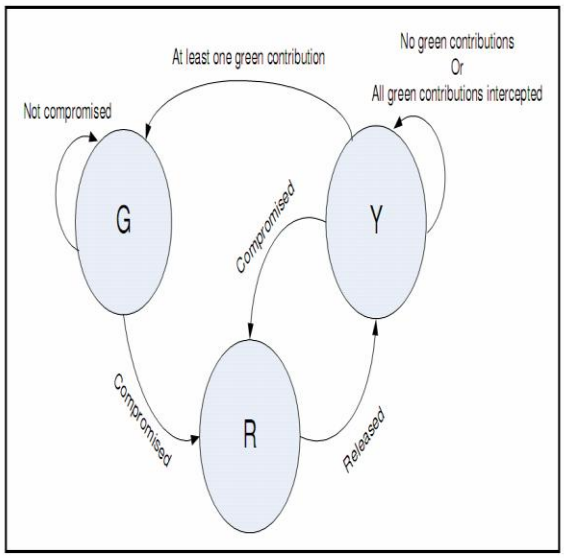

Fig 2. Transition Diagram

Adversary (ADV) is stationary with respect to the portion of the deployment area it controls; but, the set of compromised sensors changes as nodes move in and out of the adversary-controlled area.

Based on sensor compromise and the adversary knowledge of its secrets:

- Green sensors (Gr): A sensor is green if its current secrets are unknown to ADV. This is because either it has never been compromised or because it has recovered secrecy via the key-insulated protocol.
- Red sensors (Rr): A sensor is red if it is currently compromised and its secrets are exposed to the adversary.
- Yellow sensors (Yr): A sensor is yellow if it is not currently compromised, but ADV still knows its secrets for the current round.

Advantages

Node mobility helps to solve network connectivity problems caused by sensor failures and allows sensors to adapt their sampling power to respond to precise events.

- A green sensor remains green until it moves at distance less from ADV.
- A red sensor cannot become green without becoming yellow first as ADV eavesdrops on red sensors.
- A yellow sensor can become green only if it receives at least one contribution from a green sensor.

Main motive of this paper is Minimize the red sensors, Maximizing the green sensors using self healing mechanism**.**

Disadvantages

- The algorithms are used only for after adversary compromised the sensors.
- Adversary compromising cannot be avoided.

V. Results And Discussion

Both analysis and simulation results show that the collaborative protocol is effective in providing intrusion resilience in UWSNs. For small neighbourhood sizes the network exhibits a self-healing property that, with high probability, allows sensors to regain secret state as soon as they move away from the adversary-controlled regions.

This protocol is based on cooperation among sensors. The more sensors exchange random contribution, the better the resiliency performance.

IV. Conclusions

Here, there are several contributions to the UWSN. An adversary model that spreads over various areas of the deployment field. There are two novel metrics, when assessing self-healing protocols in autonomous, distributed systems. Then it has been shown that how the degree distribution of the adversary affects our self-healing protocol in a wide range of system parameters. Where a collaborative intrusion resilience protocol has been introduced and it is has been used to recover a secrets from compromised nodes from a several deployment areas while incurring a negligible overhead. Finally, thorough analysis and extensive simulation do support our findings.

References

[1] Roberto Di Pietro, Gabriele Oligeri, Claudio Soriente, Gene Tsudik, "United We Stand: Intrusion Resilience in Mobile Unattended WSNs," IEEE Transactions on Mobile Computing, vol. 12, no. 7, pp. 1456-1468, July 2013.

[2] A. Francillon and C. Castelluccia, “Code Injection Attacks on Harvard-Architecture Devices,” Proc. 15th ACM Conf. Computer and Comm. Security (CCS ’08), pp. 15-26, 2008.

[3] Nat’l Inst. of Standards and Technology, “FIPS Pub 198: The Keyed-Hash Message Authentication Code, http://csrc.nistgov/publications/fips/fips198/fips-198a.pdf, 2002.

[4] Y. Dodis, J. Katz, S. Xu, and M. Yung, “Key-Insulated Public Key Cryptosystems,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’02), pp. 65-82, 2002. [5] M. Bellare and A. Palacio, “Protecting Against Key-Exposure: Strongly Key-Insulated Encryption with Optimal Threshold,”Applicable Algebra in Eng., Comm. and Computing, vol. 16, no. 6,pp. 379-396, 2006.

[6] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Data Security in Unattended Wireless Sensor Networks,” IEEE Trans. Computers, vol. 58, no. 11, pp. 1500-1511, Nov. 2009.

[7] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Catch Me (If You Can): Data Survival in Unattended Sensor Networks,” Proc. IEEE Sixth Ann. Int’l Conf. Pervasive Computing and Comm. (PerCom ’08), pp. 185-194, 2008.

[8] D. Ma, C. Soriente, and G. Tsudik, “New Adversary and new Threats: Security in Unattended Sensor Networks,” IEEE Network, vol. 23, no. 2, pp. 43-48, Mar. 2009.

[9] R. Di Pietro, D. Ma, C. Soriente, and G. Tsudik, “POSH: Proactive Co-Operative Self-Healing in Unattended Wireless Sensor Networks,” Proc. IEEE 27th Symp. Reliable Distributed Systems (SRDS ’08), pp. 185-194, 2008.

[10] D.Ma and G. Tsudik, “Dish: Distributed Self-Healing,” Proc. 10th Int’l Symp. Stabilization, Safety, and Security of Distributed Systems (SSS ’08), pp. 47-62, 2008.

[11] R. Dutta, Y.D. Wu, and S. Mukhopadhyay, "Constant Storage Self-Healing Key Distribution with Revocation in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '07), pp. 1323-1328,2007.

[12] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Detecting Compromised Nodes in Wireless Sensor Networks," Proc. IEEE 26th Symp. Reliable Distributed Systems(SRDS '07), pp. 219-230, 2007.

[13] D. Ma and G. Tsudik, "Dish: Distributed Self-Healing," Proc. 10th Int'l Symp. Stabilization, Safety, and Security of Distributed Systems (SSS '08), pp. 47-62, 2008.

[14] R. Di Pietro, L.V. Mancini, C. Soriente, A.Spognardi, and G.Tsudik, "Catch Me (If You Can): Data Survival in Unattended Sensor Networks," Proc. IEEE Sixth Ann. Int'l Conf. Pervasive Computing and Comm. (PerCom '08), pp. 185-194, 2008.

[15] Naik, A. Arora, S. Bapat, and M.G. Gouda, "Whisper: Local Maintenance in Sensor Networks," IEEE Distributed Systems Online, vol. 4, no. 9, 2003.