International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:10, 2014

Distributed Self-Healing Protocol for Unattended Wireless Sensor Network

E. Golden Julie, E. Sahaya Rose Vigita, S. Tamil Selvi

***Abstract*—**Wireless sensor network is vulnerable to a wide range of attacks. Recover secrecy after compromise, to develop technique that can detect intrusions and able to resilient networks that isolates the point(s) of intrusion while maintaining network connectivity for other legitimate users. To define new security metrics to evaluate collaborative intrusion resilience protocol, by leveraging the sensor mobility that allows compromised sensors to recover secure state after compromise. This is obtained with very low overhead and in a fully distributed fashion using extensive simulations support our findings.

***Keywords*—**WSN security, intrusion resilience, compromised sensors, mobility.

I. Introduction

THE unattended WSN feature, this kind of WSN consisting of sensor and itinerant sink that sporadically collects perceived information is termed as unattended wireless sensor networks (UWSNs).In a UWSN, the itinerant sink roams around the sensing region and collects the information perceived by sensors [1]. Security in WSN is a more challenging problem, from all kinds of resource constraints [2]. Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital physical science have enabled the development of cheap, low-power, multifunctional sensing element nodes that are tiny in size and communicate unfettered in short distances. These small sensing element nodes, that encompass sensing, processing, and human activity elements, leverage the thought of sensing element networks supported cooperative effort of an outsized variety of nodes. Sensing element networks represent a big improvement over traditional sensors [3]. Lack of secure storage forces sensors to store crypto graphic material, like keys and seeds in regular memory.

Some recent work showed that commodity sensors may be simply compromised, even while not physical access. With compromise, the adversary will scan the sensor program memory and storage [6]. As a result, in spite of that security techniques area unit in use, sensor compromise exposes all of its secrets to associate adversary. From that moment on, any cryptanalytic protocol [8], [10] achieves to be effective. As an example, if the sensor habitually encrypts measurements employing a secret key shared with the sink via a symmetric Cryptography rule (e.g., AES), the adversary that disrupts the sensor learns the key and might decipher any cipher text made by its victim. If the secret is used for integrity functions (e.g., via HMAC) the adversary may turn out capricious measurements. Supported the time of corruption, the safety state of a given sensor may be divided in 3 states: 1) time before corruption; 2) time throughout corruption; and 3) time following corruption. Nothing may be done concerning security in state a pair of because the adversary controls the sensor, whereas implementing security in state 1 and 3 needs forward and backward secrecy, severally. A cryptanalytic protocol is forward secured if exposure of secret material at a given time does not result in compromise of secrets for any time preceding compromise [11]. Whereas, a cryptanalytic protocol is backward secure if compromise of secret material at a given time does not result in compromise of any secret to be employed in future.

TRNGs are that the presence of a trustworthy third party (TTP), this is assumed in key-insulated schemes [4], [5]. In forward and backward secrecy is achieved by having end-sensor developed their secrets in cooperation with a TTP, called a base. Unless both the end-device and the base are compromised at the same time, per-round keys are insulated. Key-insulated schemes [7] are well matched for WSNs with a constantly present sink. However, there are settings where the constant presence of a sink is not viable. If the deployment area is large or adverse an online sink might not be feasible. Moreover, if the area is hostile, a fixed sink could be a single point of failure deactivating the sink, the whole WSN becomes useless. In all these settings, the sink may be roaming entity that would rather visit the network at irregular intervals to collect sensor measurements and perform maintenance [9].

In static UWSNs, sensor collaboration was shown to be one such effective technique. Sensors exchange pseudo random contributions, i.e., values drawn from their pseudorandom variety generator, and use received contributions beside their current secrets to figure future secrets. This way, if a previously compromised sensor obtains a minimum of one random contribution unknown to the adversary, it regains secrecy. We tend to introduce general metrics to assess the effectiveness of intrusion-resilient protocols for mUWSNs and later propose a collaborative distributed protocol [8], [9] that influences sensor cooperation and movement to realize probabilistic key insulation. Sensors make the most of quality and collaboration with peers to regain secrecy when having been compromised by unknowingly wandering into the world below adversarial management. We tend to show that the

Golden Julie E. is Research Scholar with the Information and Communication Engineering, Anna University, Chennai, India (e-mail: juliegolden18@gmail.com).

Sahaya Rose Vigita E. is Assistant Professor with the Dept of M.C.A in Jain University, Bangalore. (e-mail: sahaya.r.vigita@gmail.com)

Tamil Selvi S. is Professor & Head of PG Department of ECE, National Engineering College, Kovilpatti, India (e-mail: tamilgopal2004@yahoo.co.in).

proposed protocol provides probabilistic key insulation without trustworthy third parties or secure hardware and with lowest overhead.

II. Description of the Problem

Mobility helps to resolve network property issues caused by device failures and permits sensors to adapt their sampling power to retort mounted events [12]. And mobile sensor will extend sensor life time's delivery energy to sensors with depleted batteries. Lastly, quality is presently being examined as a way to notice device capture attacks. One amongst the foremost vexing issues in wireless device network security is that the node captures attack. An adversary can capture a node from the network as a first step for further different types of attacks. As an example, the adversary will collect all the cryptographically material keep within the node. Also, the node may be reprogrammed and re-deployed within the network so as to perform malicious activities. To the simplest of our information no distributed answer has been planned to notice a node capture in an exceedingly mobile wireless device network.

The UWSN model a mobile adversary that migrates among totally different subsets of compromised sensors [12]. In our mUWSN setting, sensors are mobile whereas the adversary is static. i.e., it might as well be stationary and stay up for sensors to move to its controlled space. We tend to concentrate on the impact on self-healing of a distributed, static adversary. Our adversary (ADV) is stationary with relevancy the portion of the preparation space it controls; however, the set of compromised sensors changes as nodes move in and out of the adversary-controlled area [3]

***Adversarial Degree*:** ADV is either centralized or distributed [5]. In any case, it has an overall compromising area S_{ADV} that is partitioned into one or more equally sized non overlapping compromising regions. Each compromising region is a spherical cap with center ap_a, surface S_a, and range p_a, for $1 <= a <= 4$.

***Compromising Power*:** ADV ^{A} compromises all sensors within its range, i.e., s_j is compromised at round r if $D^o(cp^r_j, ap_a)<=p_a$, for any a<= A. For each compromised s_j, the adversary reads all s_j's storage/memory and eavesdrops on all incoming and outgoing communications. A compromised sensor is released as soon as it moves away from all the compromising regions, i.e., if $D^o(cp^r_j , ap_a)>p_a$, for all $a <= A$.

Assume that the adversary is not a global eavesdropper and can only be eavesdropper on its compromising regions. A number of techniques allowed discovering sensor compromise when the adversary modifies the sensor code. Hence, if the individual is restricted to "read-only" attacks and keeps the sensing element code unchanged, there are no thanks to tell whether or not that sensing element has ever been compromised. This permits ADV to remain unseen and enjoy recurrent attacks to the network. Finally, we have a tendency to assume that ADV is tuned in to the network defense strategy whereas neither the sensors nor the sink understand ADV's location.

To check the integrity of data transmitted over or hold on in an unreliable medium could be a prime necessity within the world of open computing and communications. Mechanisms that offer such integrity checks supported a secret key square measure typically known as message authentication codes (MACs). Typically, message authentication codes square measure used between 2 parties that share a secret key so as to attest data transmitted between these parties. This customary defines a mack that uses a cryptographical hash perform in conjunction with a secret key. This mechanism is named HMAC [7], [8].

III. Network Model

Our techniques can be applied to *m*UWSN deployed on any fixed-area surface; we assume that it reflects a single acquisition of data from the environment. Sensors obtain measurements once per round, that is, at round r sensor sj obtains data drj. The sink is an itinerant trusted party that visits the network with a certain frequency. Upon each visit, the sink obtains collected measurements from every sensor, erases sensor memory, provides a fresh initial secret seed for the PRNG, and resets the round counter to 1. Sensor sj starts at position cp0j and moves over the deployment area according to a network-wide mobility model. We consider two mobility models.

Random Jump quality Model (RJ): every sensor sets its speed thus it will reach any purpose of the sphere in one round. Beginning with round r = 1 and initial position cp0j, sj chooses a random purpose wprj and moves there atomically.

Random Waypoint Mobility Model (RP): All the sensors move with the same constant speed. At round 1, s_j at position cp^0_j chooses a random point wp^1_j and gradually moves there in $[Do(cp^0_j,wp^1j)\ /m\ ]$ rounds, where $Do(cp^0_j,wp^1j\ )$ is the orthodromic distance between $cp^0_j$and the waypoint wp^1_j. Once s_j reaches wp^1_j, it chooses a new waypoint and starts moving toward it.

Before deployment, each s_j is initialized with: 1) the sink public key PK; 2) a common cryptographic hash function H (.) used as a pseudo-random number generator (PRNG); and 3) a unique secret seed to bootstrap its PRNG [12].

IV. Distributed Self-Healing Protocol

At round r, each s_j runs Algorithm 1: It moves according to the adopted mobility model (Move ()) and after reaching its new position, senses data from the environment (Read ()).

Algorithm 1: SELF-HEALING PROTOCOL

1. Move();//Randomway-point(cp,wp,m)
2. D^r_j = Read();//Sense data
3. K^r_j = PadGen(K^r_j);//Generate new key from secret state
4. Store ($E_{PK}(K^r_j, d^r_j ,r ,s_j)$);//Encrypt &store current state
5. R^r_j =[θ];//Initialize peer contribution vector
6. C = 0;
7. t= RandGen(K^r_j);//Pick new secetseed
8. Broadcast(t);//Broadcast new secret to peers
9. While (roundTimer) do
10. Receive t^r_p from s_p;
11. $R^r_j[c] = t^r_p$;
12. C = c+1;
13. End//generate new secret state

14. $K_j^{r+1} = H(K_j^r \| R_j^r[0] \| \ldots \| R_j^r[c-1])$;
15. Delete (K_j^r, K_j^r);

V. Packet Authentication

The main purpose is to recover secrecy of their cryptographic material after compromise.

A. Process Description

This paper supported cooperation among sensors. The additional sensors exchange random contribution, the higher the resiliency performance. As a good method for a sensor to succeed in additional peers and improve randomness exchange. Yet, because the adversary eavesdrops on its compromise area(s), sensors have Associate in Nursing incentive keep a restricted communication range. In every sensor would reach all peers however, at constant time, the adversary would listen in on every contribution exchange. To unfold "healing randomness" round the network, our protocol leverages sensor quality instead of transmission range. Since sensor quality could be an intrinsic feature of mUWSNs, intrusion resilience comes at just about no cost. The utilization of public key coding permits the sink to rewrite any ciphertext, regardless of that messages were not properly changed or that sensors unsuccessful throughout the sink absence.

B. Evaluation Indicator

Generic key-insulated protocol has two new metrics: Health Ratio (H_R) and Healthy Cycle (H_C). The natural goal of any intrusion-resilient protocol is to have both H_R and H_C as close as possible to 1. In HR= 1 means that secrets of almost all sensors are not exposed

$$\text{Health Ratio} = G / G+Y \quad (1)$$

G = No of Green sensor; Y = No of Yellow sensor

$$\text{Health Cycle} = TtC / TtC + TtH \quad (2)$$

TtC = Time to Compromise; TtH = Time to Heal

C. Experimental Verification

Sensor node moves randomly and freely without having any restriction. Sink verifies the sensor node initial key for authentication.

TABLE I
Simulation Result for Health Ratio and Health Cycle

No of sensor node	Mean no of neighbor	Health Ratio	Health cycle
50	5	0.20	0.30
50	10	0.22	0.32
50	12	0.83	0.89
50	15	0.99	0.99

Fig. 1 shows that the comparison of the relationship between HR and mean number of neighbors. The number of neighbor size is high the energy of sensor transmitting power is low and Health Ratio is increased.

Routing Control Overhead: Overhead will increase the extent of disseminated unwanted data and redundant process at intermediate nodes further as base station

$$EC=D_C+T_C \quad (3)$$

where D_c is the pay expenses which are cluster coordinator node controlling according to the built path transmission cluster heads need and

T_c is multiple paths in need of the overhead of data transmission.

Fig. 2 shows the routing overhead in network. The proposed protocol performs far better than LEACH and DD. As time increases it performs better than LEACH. Routing done by DHL is responsible for the reduced routing overhead.

Longevity

The numbers of alive nodes are calculated for several simulation periods. The graph in Fig. 3 indicates that DSL ensures more number of nodes alive for the different simulation times

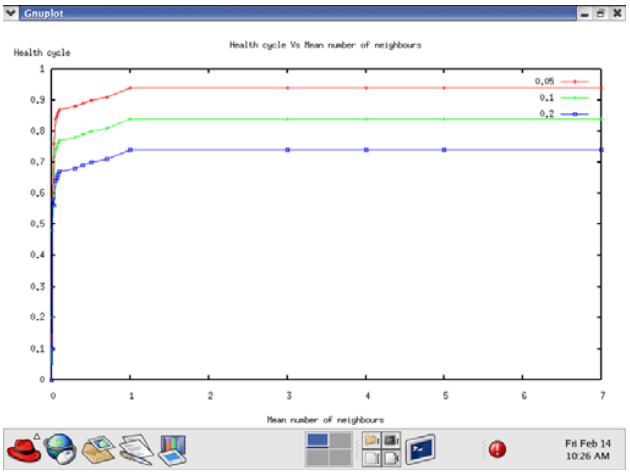

Fig. 1 Health cycle Vs Mean no of neighbors

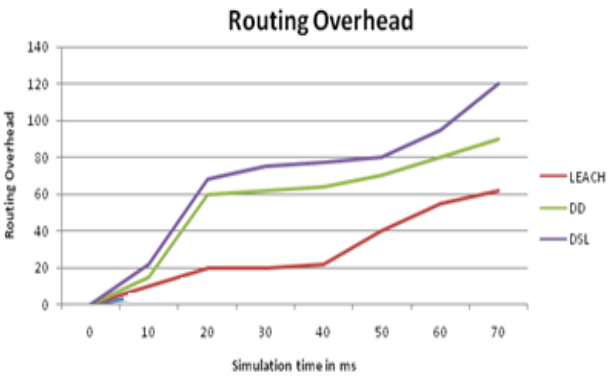

Fig. 2 Routing overhead

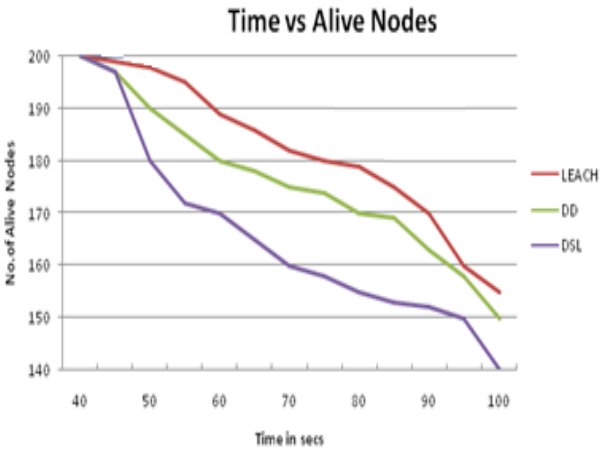

Fig. 3 Node Longevity

VI. Conclusion

This protocol provided several contributions to the UWSN field. First, to introduce a new adversary model that spreads over different areas of the deployment field. Second is to introduce assessing self-healing protocols in autonomous, distributed systems. Third for a wide range of system parameters, how the degree distribution of the adversary affects our self-healing protocol. Finally, thorough analysis and extensive simulation do support our findings.

References

[1] "Wireless sensor networks: a survey" I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, USA Received 12 December 2001; accepted 20 December 2001

[2] "Data Security in Unattended Wireless Sensor Networks" Roberto Di Pietro, Luigi V. Mancini, Claudio Soriente, Angelo Spognardi, Gene Tsudik.2009

[3] "New Adversary and New Threats: Security in Unattended Sensor Networks" Di Ma, Claudio Soriente and Gene TsudikComputer Science Department University of California, 2009

[4] "Mobility and mobility management: a conceptual framework". Proc. 10th IEEE International Conference on Networks. Retrieved 23 February 2009.

[5] "Mobility Improves Coverage of Sensor Networks" Benyuan LiuDept. Peter BrassDept. of Computer ScienceCity College of New YorkNew York, 2009

[6] "A Survey Of Mobility Models in Wireless Adhoc Networks "Fan Bai and Ahmed Helmy University of Southern California,U.S.A .2002

[7] "The Keyed-Hash Message Authentication Code (HMAC)" Information Technology Laboratory National Institute of Standards and Technology. 2010

[8] "Key-Insulated Public Key Cryptosystems"Yevgeniy Dodis1, Jonathan Katz2, Shouhuai Xu3, and Moti Yung41 Department of Computer Science, New York University.2010

[9] "Intrusion-Resilience in Mobile Unattended WSNs" Roberto Di Pietro , Gabriele Oligeri, Claudio Soriente , Gene Tsudik ISTI-CNR, Pisa Research Area, Pisa, Italy Computer Science Department, University of California, Irvine, USA.2010

[10] E.P.G.D. Murphy and W. Marnane, "Area-Efficient Processor for Public-Key Cryptography in Wireless Sensor Networks," Proc.Second Int'l Conf. Sensor Technologies and Applications.2009

[11] R. Wang, W. Du, X. Liu, and P. Ning, "ShortPK: A Short-TermPublic Key Scheme for Broadcast Authentication in SensorNetworks," ACM Trans. Sensor Networks, vol. 6, pp. 9:1-9:29, Jan.2010.

[12] V. Shoup, "OAEP Reconsidered," Proc. 21st Ann. Int'l Cryptology Conf. (CRYPTO '01), pp. 239-259, 2001.

E.Golden Julie received her B.E degree in Computer Science and Engg in 2005 from Anna University Chennai and ME degree in Computer Science and Engineering in 2008 from Anna University Chennai. Currently she is Pursuing her Ph.D from Anna University Chennai. Presently she is working as assistant professor in Regional centre Anna university, Tirunelveli, India She has published many research papers in various fields. Her research area includes Wireless Sensor Adhoc Networks and Image Processing. She is a member of ISTE

E.Sahaya Rose Vigita received her MCA degree from Madurai Kamaraj University in 1999 and M.E degree in Computer Science and Engineering in 2013 from Anna University, Chennai. Currently she is working as Assistant Professor in Jain University, Bangalore. Her areas of interest include Mobile Adhoc Networks and Wireless Sensor Networks. She has published papers in National and International Journals.

S. Tamil Selvi received her B.E. degree from Madurai Kamaraj University, in 1988, M.E. degree from College of Engineering, Guindy, Anna University, Chennai in 1997 and Ph.D. degree from Manonmaniam Sundaranar University, Tirunelveli in 2009. Presently she is working as Professor in ECE department, National Engineering College, Kovilpatti, India. Her area of interests includes wireless sensor networks and Image Processing, Wireless communication. She has published 24 papers in international journals. She is a fellow of IE (I) and IETE, life member of ISTE and CSI and annual member of IEEE.