Detection of False Data Distribution Nodes in Wireless Sensor Networks

K.Sundara Velrani
Assistant Professor
Department of CSE
Amity School of Engineering and Technology
Noida

ABSTRACT
In wireless sensor networks node compromise attack is a serious threat. Last few years many previous works has found out compromise node at the later stage. There are different stages of attacks: In first stage physically capturing and compromising nodes: Next stage compromised nodes back to the sensor networks: Last compromised sensor nodes rejoining the network and launching attack. This research work for early detection of compromised nodes in wireless sensor networks. In this work pair-based scheme to detect the node compromise attack in early stage. After sensor nodes are deployed they first build pairs in ad hoc pattern. Then the nodes within the same pairs can monitor each other to detect any node compromise attempt.

Keywords
Wireless sensor networks, node compromise attack, pair building

1. INTRODUCTION
A wireless sensor network is composed of a large number of low cost sensor nodes to perform distributed sensing tasks by interconnecting with wireless links. Each sensor node is equipped with necessary sensing, data processing and communication components. When a sensor node generates a report triggered by a special event, like a surrounding temperature change, it will report the sensed data to a data collection unit also called sink through a predefined routing. Due to the fast booming of micro electro mechanical systems, wireless sensor networking has held great promise as an enabling technology for a variety of applications such as environmental and habit monitoring [1], surveillance and tracking for military [2].

This paper committed to developing a new Pair Based node compromise Detection (PBD). Compared with previously reported schemes, the proposed PBD scheme detects the node compromise attack in the first stage. After sensor nodes are deployed in a local area, they first build pairs in ad hoc pattern. Then, the nodes within the same pair can monitor each other. Goal of this research work is to seek an alternative solution to early detect the node compromise attack.

The remainder of this paper is organized as follows. In section 2 review some related work. In section 3, also recall some backgrounds of sensor node and physical node compromise attack. In section 4, introduce the system model and design goal. Then present the proposed PBD scheme in section 5 followed by the security analysis and simulation evaluation and comparison between detection rate of Pair Based Scheme in section VI. Finally conclusion in section 7.

2. RELATED WORK
Node compromise attack is a serious threat in success of wireless sensor networks. Many methods [5]-[13] have been used to detect node compromise attack. Roughly speaking, these techniques can be categorized into two classes: detection in the second stage [5]; and detection in third stage [6]-[12]. Detection in the second stage in [5], Song et al. make the first attempt to detect node compromise in the second stage. Their motivation is that for some applications, an adversary may not be able to precisely deploy the compromised sensors back into their original positions. Then, the detection of location change will become an indication of a potential node compromise. Detection in the third stage. In [6] to handle the MAC layer misbehavior, Kyasanur and Vaidya propose modifications to IEEE 802.11 MAC protocol to simplify misbehavior detection. Once the sensor nodes are compromised, they could launch false data injection attack. Thus several en-route filtering schemes [7] [8] have been proposed to drop the false data en-route before they reach the sink. Nevertheless, these schemes only mitigate the threats. Thus in [9], ye et al. propose a probabilistic nested marking scheme to locate colluding compromised nodes in false data injection attacks. Recently several software-based attestation schemes [10] [11] for node compromise detection in sensor networks also have been proposed. However, they are not readily applied into regular sensor networks due to several limitations [12]. In [12], Yang et al. present two distributed schemes towards making software based attestation more practical. In these schemes, neighbors of a suspicious node collaborate in the attestation process to make a joint decision. Different from the above previously reported schemes, this proposed scheme attempts to detect the node compromise attack in the first stage.

3. FEATURES OF SENSOR NODE

3.1 Architecture of Sensor nodes
Sensor node shown in Fig.1 consists of sensing module, data processing module, and communicating module. Jointly fulfill the monitoring task decided by the application requirements [3]. Currently Mica2 motes are the most widely used sensor nodes, which have been adopted in many wireless sensor network installations [12]. Typically the Mica2 uses an Atmega128 chip for its processor, which is an 8-bit processor running at 4MHZ, and equipped with 128KB program memory, 4KB RAM and 4KB EEPROM. The Mica2 is programmable, which allows for not only programming but also supporting On Chip Debugging (OCD) [3].

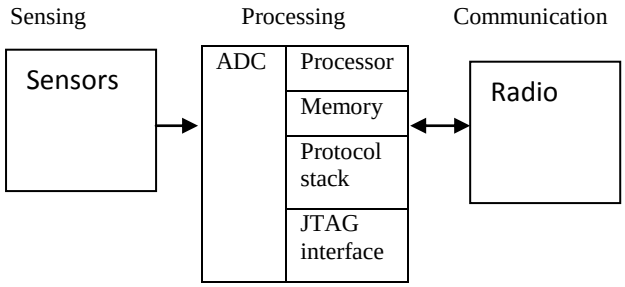


Fig 1: Sensor node inner architecture

4. SYSTEM MODELS AND DESIGN GOAL

In this section the network model, the attack model, and identify the design goal.

4.1 Network Model

Wireless sensor network which is comprised of a sink and large numbers of sensor nodes $N=\{N_1,N_2\ldots\}$uniformly deployed at a certain interested area as shown in Fig.2 The sink is a trust and powerful data collection device, which is responsible for collecting the data sensed by sensor nodes. Each sensor node Ni has a unique nonzero identifier and is stationary in allocation. The communication in the network is generality, assumed each sensor node periodically collects the sensed data and reports them to the sink via a predefined routing. In the attack model, assume that an adversary A can capture a small fraction of sensor nodes in a local area, reprogram them with malicious code, and redeploy them back into the network using the physical node compromise attack. Especially the adversary has two physical attack policies: First directly physically attack the sensor node at the sensor node's original position then firstly shut down some sensor nodes and launch physical attack at other place. Without loss of generality, assume that there are n sensor nodes in a local area, and the adversary A can only simultaneously compromise k sensor nodes in the local area, where k<n.

4.2 Design Goal

The design goal of this paper is to develop a pair-based detection scheme to early detect sensor node compromise attack. Specifically committed to addressing the node compromise problem in the first stage. To achieve the design goal, the only assumption is that each sensor node can detect being connected by a programming board when the adversary A launches the physical node compromise attack, which is very trivial for any computing device.

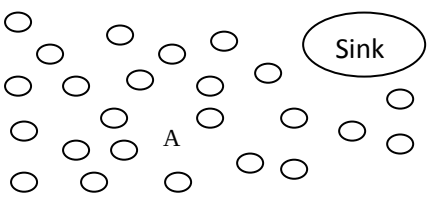


Fig 2: Wireless sensor networks under consideration

Algorithm Sensor Nodes Initialization Algorithm

1. procedure SENSOR NODES INITIALIZATION

   Input: un-initialized sensor nodes $N= \{N_0, N1...N_m\}$

   Output: initialized $N= \{N_0, N1...N_m\}$

2. for i =0 to m do
3. randomly choose a private key $x_i \in [1,r-1]$
4. compute the corresponding public key $y_i = x_i.G$
5. preload sensor node Ni with key pair(xi, yi)
6. end for
7. return initialized $N= (N_0, N_1,N_m\}$
8. end procedure

4.3 Pairs Building

In order to be armed with the capability of detecting the possible node compromise attack in the unattended area, all sensor nodes will build pairs in ad hoc mode shortly after the deployment. For example, there are n sensor nodes in a local area, two neighboring sensor nodes can form pair, one is H-node (Husband node) and the other is W-node (Wife node), as shown in Fig. 3. Suppose sensor nodes Ni, N_j are ready to build a couple, they will execute the following steps:

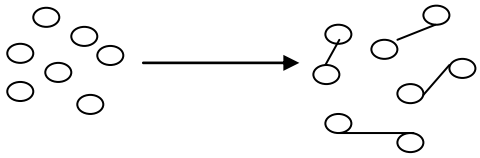


Fig 3: Building pairs (H-W nodes) in wireless sensor networks

1. Ni first chooses a random number $a \in [1, r-1]$, computes A=a.G, and sends (N_i, A) to N_j.
2. After receiving (N_i, A), N_j chooses another random number $b \in [1, r-1]$ and computes B=b.G. Then N_j uses the Naccache-Stern signature [15] to make a signature on $A||B||\ N_i$ as $N_j\ (A||B||\ N_i)$. Finally N_j sends $(N_j, B, N_j\ (A||B||\ N_i))$ back to N_i.
3. Upon receiving $(N_j, B, N_j\ (A||B||\ N_i))$, N_i checks the validity of the signature $N_j\ (A||B||\ N_i)$. If the signature is accepted N_i makes a signature on $B||A||\ N_j$ as $N_i\ (B||A||\ N_j)$ and sends the signature to N_j. At the same time, N_i computes the shared key =h (a.B) =h (ab.G), where h :{ 0, 1 is a secure hash function.
4. After receiving and checking the validity of N_i $(B||A||N_j)$,N_j also computes the shared key k_j=h (b.A) =h (ab.G). Note that, since the identities N_i and N_j are included in the signature. Once the shared key $k_i = k_j$ =h(ab.G) is established the pair nodes N_i, N_j can securely make the time synchronization operation and monitor each other by periodically sending or receiving beacon information. For example, every Interval time interval N_i computes $k_j = k_j +1$ and $Beacon_i$= h ($k_i||\ N_i||1$). Then N_i broadcasts (N_i,$Beacon_i$) within its transmission range. After receiving (N_i, $Beacon_i$) from N_i the pair node N_j will check the beacon information by first computing $k_j = k_j +1$ and comparing $Beacon_i$ h ($||k_j||N_i||1$). If it holds N_j believes N_i is not compromised. However if it doesn't hold, the node compromise attack is possible.

4.4 Sensor Nodes Compromise Attack Detection

Assume that an adversary A is physically compromising a sensor node N_i, the sensor node N_i can detect itself being connected by a programming board. Then N_i computes $k_i=k_i+1$ and sends $Beacon_i=h(k_i||N_i||0)$ to pair node N_j. After receiving Beaconi=h ($k_i||N_i||0$), the pair node N_j can detect the exception quickly by the Algorithm 2 is an exception, N_j can detect the node compromise attack. Exception I means the N_i detects itself being attached by the adversary A. When the Exception I occurs, the pair node N_j is informed that an adversary A is compromising N_i. Exception II implies that an adversary A has shut down N_i and is trying to compromise it. Note that when N_i is shut down by the adversary A, it couldn't inform its pair, while the pair N_j can detect it. It is worth noting that this is motivation to build pairs. Therefore, no matter what exception takes place, the pair N_j will broadcast the exception to its neighbors and also report it to the sink. Note that, the exception could be triggered by the noise interferences. Therefore, to reduce the false detection, a threshold value T_h is first defined. Then, only if the number of consecutive exception is larger than or equal to T_h, the pair node will report the exception.

4.5 Discussions

In the proposed pair-based detection scheme, an implicated assumption is that each sensor node in the local area can form a pair with other nodes. However due to various reasons, i.e., the number of sensor nodes n is odd or the limitation of node's transmission range, some sensor nodes become orphan nodes and can't be detected by other nodes. To avoid the existence of orphan nodes, a straightforward solution, like many existing schemes [5], is to let more than one nodes detect a single node. However this solution requires time to be synchronized within many sensor nodes. Without the accurate time synchronization, much false detection may be caused.

Algorithm 2 Detect Node Compromise Attack Algorithm

1. Procedure DETECTNODECOMPROMISEATTACK
2. If N_j receives a valid beacon $Beacon_i$ from N_i every a predefined period T_t then
3. $K_j= k_j+ 1$
4. If $Beacon_i ==h(k_j \| N_i \| I)$ then
5. Return Normal
6. else if $Beacon_i == h(k_j \| N_i \| 0)$ then
7. return Exception I
8. end if
9. else if N_j doesn't receive a valid beacon $Beacon_i$ from N_i every a predetermined period T_t then
10. return Exception II
11. end if
12. end procedure

To address the orphan nodes, introduce the hybrid pairs building, which doesn't require time synchronization in many sensor nodes. N sensor nodes can form hybrid couples in ad hoc mode, namely H-W nodes and H-W-C nodes, where "C" stands for Child node. First, n sensor nodes try to form H-W nodes. If there exist orphan nodes, some H-W-C nodes will be formed. In the H-W-C nodes mode, Husband node, Wife node and Child node, will monitor each other using Algorithm 2. Thus the orphan nodes can be eliminated in wireless sensor network.

5. SECURITY ANALYSIS

This section, discuss security issues in regard to the proposed pair-based detection scheme. The shared key ab.G established in pair building phase is secure. In the key establishment protocol, embed the identities of N_i and N_j use the Naccache-Stern signature [15] to authenticate the validity of a.G and b.G. Thus, the main-in-the middle attack can be resisted. At the same time, due to the hardness of elliptic curve computational Diffie-Hellman problem, the shared key ab.G is only known by N_i and N_j. The pair-based detection scheme can resist the replay attack. Since only the pair nodes N_i and N_j know the shared key ab.G and the one-wayness of hash function h (), it is hard for an adversary A to get the ab.G. Then if an adversary launches the relay attack, it can be immediately detected. With the above security guarantees, the pair-based detection scheme can be applied to detect the physical sensor node compromise attack.

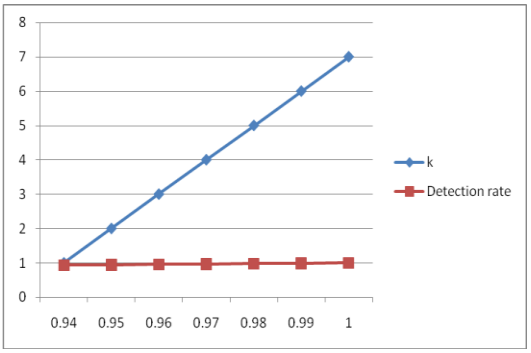
6. EXPERIMENTAL RESULTS

This section evaluates the proposed pair-based detection scheme in terms of detection rate i.e., the probability to successfully detect the sensor node compromise attack. Concretely will analyze the detection rate of the proposed scheme via experiments conducted on a customized NS2-Simulator.

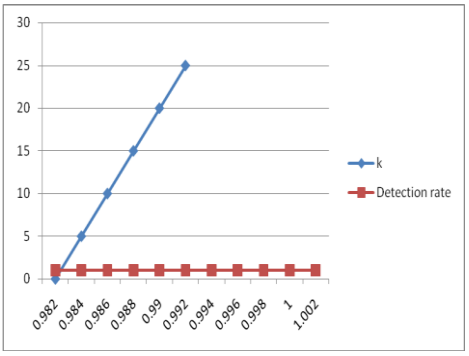
6.1 Simulation Environment

In the simulations, n sensor nodes with a transmission radius of 20m are randomly deployed in a restricted 50 m ×50m local area. The tunable parameters in the simulation are given as follows:

- The number of sensor nodes n, which is varied from 10 to 25.
- The interval of beacon information interval, which is set as 2 seconds, 4 seconds, 8 seconds and 12 seconds.
- The threshold value of exception detection T_h, which is varied from 1 to 3 in increment of 1.
- The time of an adversary A successfully compromises a sensor node T_c, which is varied from 30 seconds to 60 seconds. Test the networks with different parameter settings. For each case, 10000 networks are randomly generated, and the average detection delay over all of this randomly sampled network is reported.



n=10



n=25

Fig 4: Detection rate varies with k under different n=10, 25 Interval=2s, and T_h=1

6.2 Comparison between detection rate of Pair-Based Scheme

Table 1. Finding Stage

Scenarios	Pdata	Detection Rate	Stage
1N	0,10	0(for all)	Third
5N	0,10	100%(for all)	Second
10N	0,10	100%(for all)	First
15N	0,30	50%,50%	First
20N	0,30	50%,50%	First
25N	0,30	50%,50%	First

Table 1 shows 1N find out compromise attack in the third stage, 5N find out compromise attack in the second stage and 15 to 25N find out in first stage itself. Detection Rate various in each scenarios. 5N and 10N give 100% detection rate and remaining gives 50% detection rate.

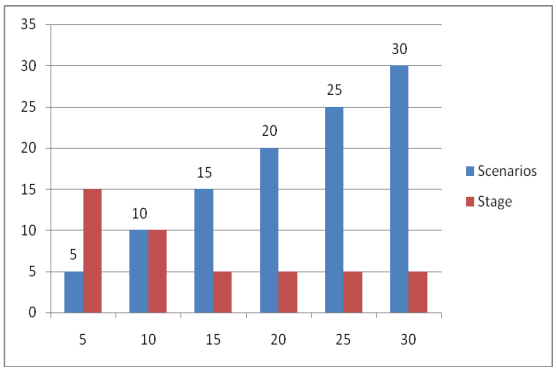


Fig 5: Detect the node compromise attack in different stage

7. CONCLUSIONS

In this paper the proposed pair-based detection scheme to early detect the node compromise attack in the first stage. Concretely, by simply building pairs among neighboring sensor nodes in a local area, physical node compromise attack can be detected immediately. The simulation results show that the proposed pair-based detection scheme has high detection rate. As an initial work, just have shed light on detecting compromise attack in the first stage, and do not expect the proposed scheme to solve all problems in the node compromise attack. My future work will continue to validate different pair buildings and their effects on the detection of node compromise attack in wireless sensor networks.

8. REFERENCES

[1] R.Szewczky, A.Mainwaring, J.Anderson, and D.Culler,"An analysis of a large scale habit monitoring application," in Sensys'04, 2004.

[2] L.Eschenauer and V.D.Gligor, "A key-management scheme for distributed sensor networks," in ACM CCS'02, 2002.

[3] C. Hartung, J. Balasalle, and R.Han, "Node compromise in sensor networks: the need for secure systems," in Technical Report CU-CS-990-05, Dept. of Comp Sci. Univ of Colorado at Boulder, Jan 2005.

[4] V.C. Giruka, M.Singhal, J.Royalty and S.Varanasi," Security in wireless sensor networks", Wireless Communications and Mobile Computing, Vol.8, No.1, pp.1-24, 2008.

[5] H.Song, L.Xie, S.Zhu and G.Cao, "Sensor node compromise detection: the location perspective," in IWCMC'07, Honolulu, Hawaii, USA, Aug. 2007.

[6] P.Kyasanurand H.Vaidya, "Detection and handling of mac layer misbehavior in wireless networks," in IEEE DSN, 2003.

[7] S.Zhu, S.Setia, S.Jajodia, and P.Ning,"An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in IEEE Symposium on Security and Privacy'04, 2004.

[8] H.Yang, F.Ye, Y.Yuan, S.Lu, and W.Arbaugh,"Toward resilient security in wireless sensor networks, "in ACM MobileHoc'05, 2005.

[9] F.Ye, H.Yang, and Z.Liu,"Catching moles in sensor networks," in IEEE ICDCS'07, Jun.2007.

[10] A.Seshadri, M.Luk, E.Shi, A.Perrig, L.Van Doorn, and P.Khosla, "Pioneer: verifying integrity and guaranteeing execution of code on legacy platform," in SOSP, oct.2005.

[11] D.Spinellis,"Reflection as a mechanism for software integrity verification," in ACM Trans. Inf. Syst. Secu., Vol.3, No, 1, 2000.

[12] Y.Yang, X.Wang, S.Zhu, and G.Cao, "Distributed software based attestation for node compromise detection in sensor networks," in IEEE SRDS, October 2007.

[13] A. Liu and P.Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in IPSN 2008, SPOTA Track, pp.245-256, April 2008.

[14] H.Wang and Q.Li,"Efficient Implementation of Public Key Cryptosystems on Mote Sensors," in International Conference on Information and Communication Security (ICICS), Raleigh, NC, Dec. 4-7, 2006.

[15] D.Nacache and J.Stern,"Signing on a Postcard," in Financial Cryptography-FC 2000, LNCS 1962, pp.121-135, Springer-Verlag, 2001.

[16] X.Du, Y.Xiao, M.Guizani, and H.Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Networks 2007; 5(1); 24-34.

[17] D.Liu and P.Ning, "Establishing pairwise keys in distributed sensor networks", in CCS 2003, Washington D.C., USA, Oct.2003, pp.52-61.

[18] Karlof, C., Wagner, D., 'Secure routing in wireless sensor networks: attacks and countermeasures'. Proc. First IEEE Int. Workshop on Sensor Network Protocol and Applications, 2003, pp.113-127.

[19] Wood, A.D., Stankovic, and J.A.; 'A taxonomy for denial-of-service attacks in wireless sensor networks', 'Handbook of sensor networks: compact wireless and wired sensing systems; 2004.

[20] Zhang, Y.Liu, W., Lou, W., Fang.Y.'Location –based compromise-tolerant security mechanisms for wireless sensor networks', IEEE J.Set Area Commun., 2006, 24(2), pp.247-260.

[21] Brooks,R.Govindaraju, P.Y.Pirretti,M.Vijayakrishnan, N.Kandemir,M.T:'On the detection of clones in sensor networks using random key predistribution', IEEE Trans. Syst., Man., Cybern., Part C: Appl.Rev.,2007,37(6) ,pp 1246-1258.

[22] Parno, B., Perrig, A.Gligor, V.'Distributed detection of node replication attacks in sensor networks'. Proc. IEEE Symp.on Security and privacy, 2005, pp.49-63.

[23] Choi, H.zhu, S.'La Porta TF.SET: Detecting node clones in sensor networks'. Proc.Third Int.Conf. on Security and Privacy in Communications Networks and the Workshops, 2007, pp-341-350.

[24] Kathirvel, A. and Srinivasan.R (2010) 'Self_USS: self umpiring system for security of mobile adhoc networks', International Journal of Engineering and Information Technology, Vol.2, pp.196-203.

[25] Behnke et. al 'Exploiting malicious node detection for life time extension for WSN', in 2009 Fourth IEEE International Symposium on Electronic Design, Test and Application.