Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference
on Electrical Engineering
ICEENG 2012

An Efficient Overlapped Groups based Compromised Nodes Detection at First Stage for WSN

By

Mohamed Helmy Megahed* Prof. Dimitrios Makrakis**

Abstract:

Surveillance WSNs are deployed in hostile environments such as perimeter, border locations and battlefields to detect unauthorized intrusions. Therefore, Surveillance WSNs are highly vulnerable to collaborative work of attackers to compromise many legitimate nodes. Securing surveillance WSNs is challenging because of low-cost, limited capabilities, resource-constrained sensor nodes. Several protocols have been proposed for detecting compromised nodes. However, some protocols rely on an implicit assumption that compromised node will change its location or its signal strength will alter after it is compromised; other protocols use alert messages or reputation based trust models which require the nodes misbehavior to discover the compromised nodes. Node compromise attack is a multi-stage attack which consists of three stages: physically capturing and compromising sensor nodes; redeploying the compromised nodes back to network and compromised sensor nodes rejoining the network. Our work studies how to achieve high resiliency against an increasing number of compromised nodes in large surveillance WSN in hostile environment by collaborative work of attackers at the first stage. Specifically, after sensor nodes are deployed they first build overlapped groups in ad hoc pattern where a group is composed of four nodes. Then, the nodes within the overlapped groups can monitor each other to detect any node compromise attempt. We describe the building blocks that can be used to build the protocol for the detection process. Our protocol is designed to be resistant against large number of compromised nodes by collaborative work of attackers. Extensive simulation results are given to demonstrate the high detection rate of the proposed scheme.

Keywords:

Overlapped groups; Wireless Sensor Network; Node Compromise Attack; Surveillance

* Egyptian Armed Forces, mmega080@uottawa.ca
** School of Information Technology and Engineering, University of Ottawa, Ottawa, Canada, dimitris@site.uottawa.ca

1. Introduction:

Wireless sensor networks (WSNs) are deployed in many missions' critical applications such as surveillance [1], and one of the key issues to the success of their mission is security. The general objective of such an application is to alert the control unit in advance to the occurrence of events of interest in hostile regions. The event of interest varies according to the mission type which might be the presence of moving vehicles or target detection or other events. There are several types of sensors such as Vibration, Motion, Tracking, Video, and Infrared sensors which can be used for surveillance applications [2]. With their deployment, various novel security attacks have appeared. The aims of these attacks are usually to compromise nodes, eavesdropping for traffic analysis, destroy base station (BS) or to disrupt data flow. We believe that, collaborative work of attackers will launch compromise nodes attacks against the surveillance WSN to compromise many legitimate nodes and to destroy the deployed network security.

Surveillance WSNs are usually deployed at unattended or hostile environment. Therefore, they are vulnerable to the node compromise attack [3]. A node compromise attack is a three stage attack. In the first stage, the attacker captures some sensor nodes from the network and then compromises these nodes. In the second stage, these compromised nodes are redeployed into the network. In the third stage, the attacker will use these compromised nodes to launch various security attacks. Much work has tackled the node compromise attack [4]-[18]. However, all of them address the node compromise attack either in the second stage based on node redeployment detection [4] or in the third stage based on node misbehavior detection [5]- [11]. We believe that group of attackers will launch node compromise attack to jeopardize the whole network in few minutes. Therefore, early detection of node compromise attack can lead to a more effective defense against collaborative work of attackers.

In [12] Xiaodong made the first attempt to detect node compromise in the first stage. He described a new couple based compromised node detection protocol to build couples of sensor nodes in ad-hoc pattern to detect node compromise attack at the first stage. The nodes within the same couple can monitor each other. This protocol assumes each sensor node can detect being connected by a programming board during the attack, then the node will send a message to its couple identifying that it is compromised. This protocol cannot be used against collaborative work of attackers to compromise large number of nodes where attackers can collect the couples at the same time. Furthermore, Xiaodong did not explain the path from the couple of the compromised node to the base station to report the compromised node attack where this path is critical to send the message of compromised node attack from the couple to the base station.

Our focus in this work is to achieve high resiliency against node compromise attack by collaborative work of attackers at the first stage.

To the best of our knowledge, there has not been work done for securing the surveillance WSN at the first stage from collaborative work of attackers to compromise many legitimate nodes at the same time. Therefore, for mission critical applications such as surveillance WSN, we propose to address this problem through employing our new designed overlapped groups-based compromised node detection protocol.

In this paper, we developed a new overlapped groups-based node compromise detection scheme. Compared with previously reported schemes, the proposed scheme detects the node compromise attack by collaborative work of attackers at the same time in the first stage. Specifically, after sensor nodes are deployed, they first build overlapped groups in ad hoc pattern. The group is composed of four nodes and the nodes are connected in closed loop as shown in Figure 1. Then, the nodes within the overlapped groups can monitor each other.

Objective of this paper is to present a novel node compromise detection scheme against collaborative work of attackers working at the same time in the first stage. Our motivation is the high probability of node compromise attack by collaborative work of attackers to render the whole network ineffective. Our goal is to design new node compromise detection scheme for surveillance WSN in hostile environment.

Contributions of this work can be summarized as:

The **first contribution** is the development of the new security architecture called Surveillance Security (SurvSec) for node compromise detection of surveillance WSN.

The **second contribution** is the formation of overlapped groups to allow each group to monitor its overlapped groups.

The **third contribution** is the early detection of node compromise attack at the first stage.

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 describes the assumptions of the proposed scheme. Section 4 describes an overview of our security architecture SurvSec with its ingredients. Section 5 presents the security analysis. Section 6 presents the simulation results. Finally, Section 7 concludes the paper.

2. Related Work:

We need an effective security scheme to identify compromised nodes in a timely manner because compromised nodes in surveillance WSN represent uncovered areas. A node compromise attack involves three stages. From [4]-[11], the authors proposed many protocols to detect compromised nodes based on location, signal strength, reputation, weighted trust, intrusion detection and MAC layer misbehavior. However, these approaches are not effective since they can detect compromised nodes on the second or the third stage and they depend on node's misbehavior or node's location, which means a node may be compromised but behaves well until a programmed time. In [12], a couple based compromised node detection protocol is proposed to build couples of sensor nodes where the couple can monitor each other but this scheme cannot be used against collaborative work of attackers to compromise large number of nodes because attackers can collect the couples at the same time.

Also, software-based attestation techniques [13]-[18] have been proposed to verify the contents of the code running on nodes where the node's free memory space is filled with incompressible random noise known to the attester. These techniques use a challenge-response protocol between a trusted verifier and nodes. A verifier generates a challenge which is a random number and sends it to a suspected node. When receiving this challenge, the node traverses its memory in a pseudorandom fashion and recursively computes a cryptographic checksum over each traversed memory space, and then sends the final checksum to the verifier. The verifier can verify the result since it knows the expected memory image of a legitimate node. Software-based attestation techniques based on the base station as verifier will incur large secure communications overheads with all the nodes for testing the whole network [18] and also the base station could be a single point of failure.

For the detection in the second stage: In [4], Song et al. made the first attempt to detect compromise node in the second stage. They assume that an adversary will 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.

For the detection in the third stage: In [3], Carl et al. demonstrate the case in which nodes can be compromised in the third stage and they show exactly what information can be obtained and how it can be used to disrupt, falsify data within, or eavesdrop on sensor networks. They suggest that sensor nodes in hostile environment would be desirable not to respond to the standard on-chip debugging and if a node can detect its own movement by either accelerometers or GPS then it can preemptively delete important information stored in SRAM, flash, or anywhere else on the system. Their work implies very high cost for large distributed network.

In [5], Kyasanur and Vaidya propose modifications to IEEE 802.11 MAC protocol to simplify misbehaviour detection. Once the sensor nodes are compromised, they will launch false data injection attack. Thus, several en-route filtering schemes [6], [7] have been proposed to drop the false data en-route before they reach the sink. Nevertheless, these schemes only mitigate the threats. Thus in [8], 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 [9], [10] for node compromise detection in sensor networks have been proposed. However, they are not readily applied into regular sensor networks due to several limitations [11]. In [11], Yang et al. present two distributed schemes towards making software-based attestation more practical. In these schemes, neighbours of a suspicious node collaborate in the attestation process to make a joint decision.

3. Network Assumptions, Attack Model and Design Goal:

In this section, we formulate the network assumptions, the attack model and the design goals.

3.1 Network Assumptions

We consider the following assumptions in our network model:

1- The WSN is composed of a base station and large number of sensor nodes uniformly deployed at a certain area. The base station is a trust and powerful data collection device which is responsible for collecting the data sensed by sensor nodes. Each sensor node has a unique nonzero identifier and is stationary in a location.

2- The WSN forms overlapped groups where each group is formed of four sensor nodes. Each group is overlapped with other groups by one sensor node as shown in Figure 1.

3- The communication in the network between sensor nodes in the group is formed by a closed loop. Each two groups are overlapped in one sensor node. We assume each sensor node periodically collects the sensed data and reports them to the base station via a predefined routing.

4- A group of attackers will collaboratively launch node compromise attack against the deployed surveillance WSN to reprogram the sensor nodes with malicious code then the group of attackers will redeploy the compromised sensor nodes back.

5- Each sensor node can detect being connected by a programming board when the adversaries launch the physical node compromise attack.

3.2 Attack Model

In the attack model, we assume that a group of attackers can capture large number of sensor nodes at the same time in a local area, reprogram them with malicious code, and redeploy them back into the network using the physical node compromise attack. Specifically, the attackers have two physical attack policies: 1) directly physically attack the sensor node at the sensor node’s original position; 2) firstly shut down some sensor nodes and launch physical attack at other place. Also, we assume that there are *n* sensor nodes in a local area, and the attackers can compromise *k* sensor nodes at the same time in the local area where *k* is from 2 to 5 sensor nodes at the same time.

3.3 Design Goal

The design goal of this paper is to develop overlapped groups-based detection scheme to early detect sensor node compromise attack. To achieve the design goal, we assume that each four nodes are connected in a group and each group shares other groups in one sensor node as shown in Figure 1. Therefore, when the attackers launch the physical node compromise attack against a group the other groups that share the attacked group will report this attack to the base station.

4. Overview of the Security Architecture:

In this section, we describe the overlapped groups based detection scheme in detail to early detect sensor node compromise attack. Specifically, we will address the node compromise problem in the first stage. The overlapped groups based detection scheme consists of three phases: sensor node initialization and deployment phase, forming groups phase and sensor nodes compromise detection phase.

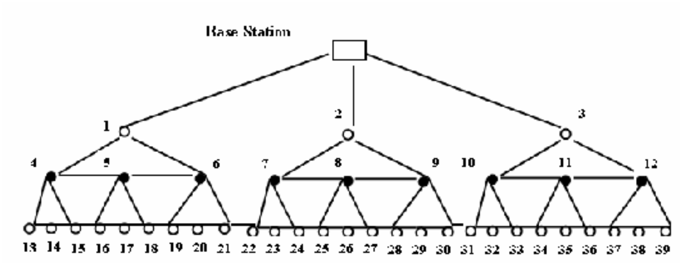


Fig. 1 SurvSec Overlapped Groups-based Compromised Node Detection Protocol Network Setup for 39 Nodes

Figure 1 describes the network setup for the proposed protocol where the nodes near the base station as nodes 1, 2 and 3 are connected to the base station and can transmit and receive beacons from the base station. Nodes 1, 4, 5 and 6 will form a group of four nodes. Nodes 2, 7, 8 and 9 will form a group of four nodes. Nodes 3, 10, 11 and 12 will form a group of four nodes. Also, nodes 4, 13, 14 and 15 will form a group of four nodes. Also, nodes 5, 16, 17 and 18 will form a group of four nodes. Also, nodes 6, 19, 20 and 21 will form a group of four nodes. Node 15 is connected to node 16 to form overlapped groups at the last layer of groups. Also, node 18 is connected to node 19 to form overlapped groups at the last layer of groups and node 21 is connected to node 22 to form overlapped groups.

4.1 Sensor Node Initialization and Deployment

The base station has the network topology of all of the sensor nodes and their locations. All the sensor nodes are initialized with a wide network key. Each sensor node in the network has a unique nonzero identifier N_i. We assume that all the sensor nodes will be almost uniformly distributed in an interested area after deployment. As a result, each sensor node will have multiple neighbors and neighbors can communicate with each other after forming overlapped groups.

4.2 Forming Groups

4.2.1 Methodology to build the overlapped groups

In this section, the methodology to build the overlapped groups is presented:

1- An overlapped group can be at least three nodes where three nodes can form a group.

2- From the network topology the base station divides the network into overlapped groups where base station first sends to the first layer of sensor nodes of nodes 1, 2 and 3 then to the second layer of sensor nodes of nodes 4, 5, 6, 7, 8, 9, 10, 11, and 12 and so on.

3- Base station sends to node 1 its group of nodes 4, 5 and 6. Also, base station sends to node 2 its group of nodes 7, 8 and 9. Furthermore, base station sends to node 3 its group of nodes 10, 11 and

12. Nodes 1, 2 and 3 are group leaders. Also, nodes 4, 5, 6, 7, 8, 9, 10, 11, and 12 are group leaders. Base station sends to every group leader its group of nodes.

4- The group leader in each group sends to each node in its group its connected nodes to form the group. Where node 1 sends to node 6 to communicate with node 5 and 1, node 1 sends to node 5 to communicate with node 6 and 4 and node 1 sends to node 4 to communicate with node 5 and 1.

5- A group can be closed group or open group if one sensor node is compromised in the group.

6- Each node is connected to maximum of four nodes.

7- As shown in Figure 1, each node near the base station as nodes 1, 2 and 3 will form a group from its downstream nodes as nodes 4, 5, 6, 7, 8, 9, 10, 11 and 12. Then, each node of the nodes 4, 5 and 6 from the first group will form a group from its downstream nodes as nodes 13, 14, 15, 16, 17, 18, 19, 20 and 21. Also, each node of nodes 7, 8 and 9 from the second group will form a group from its downstream nodes as nodes 22, 23, 24, 25, 26, 27, 28, 29 and 30. Also, each node of nodes 10, 11 and 12 from the third group will form a group from its downstream nodes as nodes 31, 32, 33, 34, 35, 36, 37, 38 and 39.Each node of the first group as nodes 4, 5 and 6 is connected to other groups which will form overlapped groups. Also, the last layer of groups as group formed from nodes 4, 13, 14, and 15 is connected to group formed from nodes 5, 16, 17 and 18 which will form overlapped groups. Our protocol will form overlapped groups.

8- From the first group, node 1 will send and receive from base station, node 4 and node 6. Also, node 4 will send and receive from nodes 1, 5, 15 and 13. Also, node 5 will send and receive from nodes 6, 4, 16 and 18. Also, node 6 will send and receive from nodes 1, 5, 19 and 21 and son on in the other groups.

4.2.2 Building the Session Keys for Each Group

In this section, the session key for each group for the proposed protocol is presented. It is composed of two phases: a key pre-distribution phase and network initialization phase. The proposal has been designed to be very light-weight because it only makes use of hash functions and symmetric encryption and does not require expensive public key operations. In this way, the proposed scheme is efficient and by orders of magnitude faster than public key schemes.

Key pre-distribution phase:

The network manufacturer during this phase generates and securely uploads each sensor node with a network wide symmetric master key KM. Such a key should be long enough to defeat brute force attacks, i.e., a minimum of 128 bits.

Network initialization phase:

This phase takes place during network deployment in the operational environment where every node discovers its group neighbors. The steps to be performed by every node are:

(1) Every node *i* generates its unique symmetric key, k_{enc}^{i}, called the node encryption key. This key is calculated by generating a random number r_i ,and performing the hash of the master key with the random number as follows: $k_{enc}^{i} = \mathrm{h}\left(k_M, r_i\right)$. For example, the encryption key for node A would be calculated as: $k_{enc}^{A} = \mathrm{h}\left(k_M, r_A\right)$.

(2) Each node broadcasts its random value, r_i, for a short period of time, that can be as short as a few seconds. A reasonable value could be about a minute. In this way, an attacker who is listening to the broadcast traffic just obtains random values.

(3) Each node receives the random values from its group neighbors and calculates their encryption keys by using the common master key. At this point, each node stores a list of pairwise keys of its group neighbors' nodes.

(4) As a result of this phase, each node stores its own encryption key and the set of pairwise encryption keys of its group neighbors' nodes.

(5) At this point, nodes can start to communicate with others using the pairwise encryption keys.

4.2.3 Sharing the Secret Keys between Groups

As shown in Figure 1, node 1 at the first group will store three keys shared with the base station, node 4 and node 6. Also, node 4 at the first group will store four keys shared with node 1, node 5, node 13 and node 15. Also, node 5 at the first group will store four keys shared with node 4, node 6, node 16 and node 18. Also, node 6 at the first group will store four keys shared with node 1, node 5, node 19 and node 21. Furthermore, node 13 will store two keys shared with node 4 and node 14. Also, node 14 will store two keys shared with node 13 and node 14. Also, node 14 will store three keys shared with node 15, node 13 and node 6.
Therefore, each group can communicate with its overlapped groups.

4.3 Sensor Nodes Compromise Attack Detection

In order to detect the possible node compromise attack in the unattended area, all sensor nodes will build groups in ad hoc mode shortly after the deployment. For example, there are n sensor nodes in a local area; four neighboring sensor nodes can form a group as shown in Figure 1. Suppose sensor nodes 1, 4, 5, and 6 are ready to build a group, they will execute the following steps in the following mathematical algorithm.

Mathematical Algorithm:

- Step 1: Sensor node 1 first generates a random number r_1 and broadcasts its random value for a short period. Sensor node 1 will generate its unique symmetric key k_1 by performing the hash of the master key with its random number.
- Step 2: Sensor node 4 and the base station will receive this random number r_1. Upon receiving this random number r_1, sensor node 4 and the base station will generate the key k_1 by performing the hash of the master key with r_1. Senor node 4 generates another random numbers r_4, and the base station generates another random number r_b. Sensor node 4 will generate its unique symmetric key k_4 by performing the hash of the master key with its random number. Base station will generate its unique symmetric key k_b by performing the hash of the master key with its random number.
- Step 3: Sensor node 1 will generate the key k_4 by performing the hash of the master key with r_4.
- Step 4: Once the shared keys are established between sensor node 1 and sensor node 4, sensor node 4 and sensor node 5, sensor node 5 and sensor node 6, and sensor node 6 and sensor node 1, the nodes in the group can securely make the time synchronization operation and monitor each other by periodically sending/receiving beacon information.
- Step 5: every time interval, each sensor node in the group computes the key $k_i = k_i + 1$ and Beacon$_i$ = h$\left(k_i \| N_i \| 1\right)$ where N_i is the sensor node unique nonzero identifier and the one represents the status of the sensor node as good. Then, each sensor node in the group will broadcast (N_i, Beacon$_i$) within its transmission range.
- Step 6: Each sensor node builds one table according to its connected nodes. This table is used to determine the sequence of reception from other nodes. After node 4 broadcasts its beacon, it will receive from node 1 in the first time interval then from sensor node 5 in the second time interval then from sensor node 15 in the third time interval then from sensor node 13 in the fourth time interval then again from sensor node 1 in the fifth time interval and so on.
- Step 7: After receiving (N_i, Beacon$_i$) from N_i, the received node will check the beacon information by first computing the k_j= k_j + 1 and comparing Beacon$_i$ = h$\left(k_i \| N_i \| 1\right)$ and the one represents the status of the sensor node as good. If it holds, the received node belives that N_i is not compromised.

However, if it doesnot hold, the node compromise attack is possible and the received node will inform the base station that sensor node N_i is compromised.

- Step 8: Assume that the attackers are physically compromising number of sensor nodes, the compromised sensor nodes can detect itself being connected by a programming board. Then, the compromised sensor nodes compute $k_i = k_i + 1$ and broadcast $Beacon_i = \left(k_i \| N_i \| 0\right)$ to other sensor nodes where zero indicates that the node itself is compromised. After receiving $Beacon_i = \left(k_i \| N_i \| 0\right)$, the received node can detect that the transmitted node is compromised.

Also, when the transmitted node is shut down by the adversary, the received node will not receive the beacon information from this transmitted node. Therefore, the received node will mark this node as compromised.

The received node will send the information of compromised node attack to the base station.

4.4 Discussions

In the proposed overlapped groups-based detection scheme, an implicated assumption is that each four nodes in the local area can form overlapped group with other groups. However, due to various reasons, the number of sensor nodes in the group can be any number but not multiple of 4.

To address this problem, we limit the usage of the scheme to be used for number of sensor nodes more than four sensor nodes.

For 5 Nodes: we divide the nodes into group of 3 nodes and another group of 3 nodes. The group of 3 nodes is overlapped with the other group of 3 nodes by one sensor node.

For 6 Nodes: we divide the nodes into group of 3 nodes and another group of 4 nodes. The group of 3 nodes is overlapped with the other group of 4 nodes by one sensor node.

For 7 Nodes: we divide the nodes into group of 4 nodes and another group of 4 nodes. The group of 4 nodes is overlapped with the other group of 4 nodes by one sensor node.

The overlapped groups-based detection scheme can be used for different beacon intervals. This beacon interval can be set to 2, 5, and 7 seconds where a node can be connected to a maximum of four nodes. Therefore, if the beacon interval is set to 7 seconds, the node will receive from the same node after maximum of 28 seconds which is less than the time to compromise a node which is 30 seconds.

From Figure 1, if node 1 is compromised, node 4 and the base station will report that node 1 is compromised.

- If node 4 is compromised, node 5, node 13, node 15 and node 1 will report that node 4 is compromised through node 21 and node 1 to the base station.
- If node 1 and node 4 are compromised, the base station will report that node 1 is compromised then node 5, node 13, and node 15 will report that node 4 is compromised through node 21 to the base station.
- If node 1, 4 and 5 are compromised, the base station will report that node 1 is compromised then node 13 and node 15 will report that node 4 is compromised through node 21 to the base station then node 6, node 16 and node 18 will report that node 5 is compromised through node 21 to the base station.
- If node 1, 4, 5 and 6 are compromised, the base station will report that node 1 is compromised then node 13 and node 15 will report that node 4 is compromised through node 21 to the base station then node 16 and node 18 will report that node 5 is compromised through node 21 to the base station then node 19 and node 21 will report that node 6 is compromised through node 21 to base station.
- If node 1, 4, 5, 6 and 13 are compromised, the base station will report that node 1 is compromised

then node 15 will report that node 4 is compromised through node 21 to the base station then node 16 and node 18 will report that node 5 is compromised through node 21 to the base station then node 19 and node 21 will report that node 6 is compromised through node 21 to the base station then node 14 will report that node 13 is compromised through node 21 to the base station.

- If node 1, 4, 5, 13, 14 and 15 are compromised, the base station will report that node 1 is compromised then node 6 will report that node 4 and node 5 are compromised through node 21 to the base station then node 16 will report that node 13, 14 and 15 are compromised through node 21 to the base station.
- If node 1 and 21 are compromised, the data cannot be sent from the entire left branch to the base station. Therefore, there must be a database at the base station to mark the compromised branch based on the input of compromised nodes where the entire left branch must be marked as compromised from the network topology.

5. Security Analysis:

In this section, we will discuss the security issues in regard to the proposed overlapped groups-based compromised nodes detection scheme. As we will see in the following, our proposal has been designed to be resistant to node compromise attack by collaborative work of attackers, and man-in-the-middle attack.

a. Perfect resilience against node capture by collaborative work of attackers: our scheme is very resistant against this attack.
b. The shared keys established between sensor nodes in the group are secure against man-in-the-middle attack: each node has its own symmetric key for authentication therefore; the man-in-the-middle attack can be resisted.

6. Simulation Results:

6.1 Simulation Environment:

We built a model for the proposed design and we implemented a simulator in MATLAB that can scale to thousand of nodes. In this simulator, sensors can send and receive data from each other's. The simulation verifies the correctness and the feasibility of our security architecture. It is our future work to implement SurvSec in some sensor network testbeds with all its ingredients. Our simulation scenarios include N nodes distributed randomly. We choose N as 1.000 sensor nodes.

The followings are the built models for simulation:

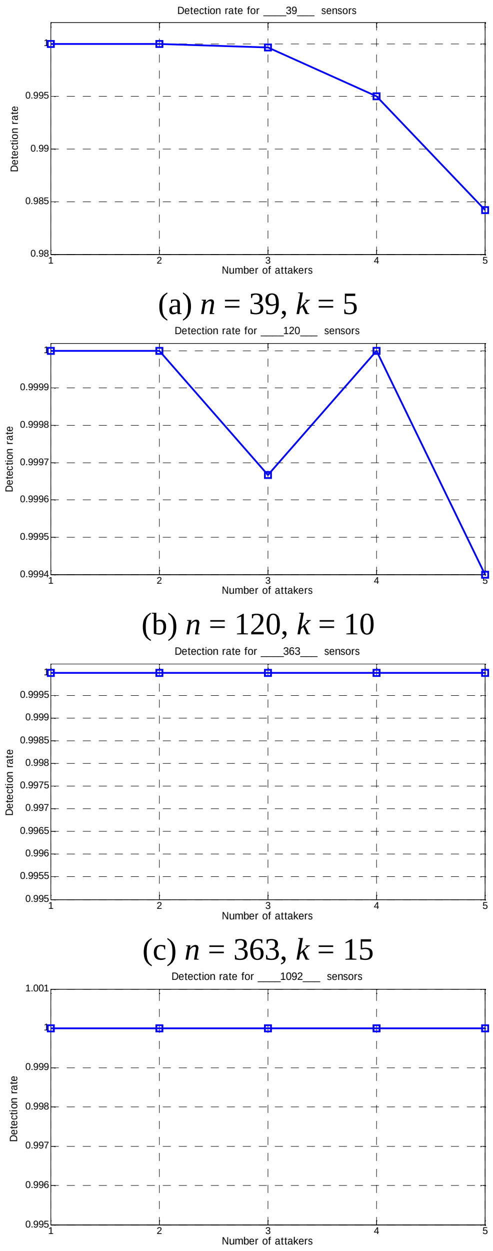
1- Network setup model for the overlapped groups.
2- Attackers' model.
3- Compromised nodes detection protocol.

In the simulations, these parameters are given as follows:

1- The number of sensor nodes *n* is varied from 39 to 1.000 sensor nodes.
2- The interval of beacon information is set to 2 seconds, 5 seconds, and 7 seconds.
3- The time of an adversary to successfully compromise a sensor node is varied from 30 seconds to 60 seconds.

Simulation Results:

In this section, we evaluate the detection rate under different n.



(a) n = 39, k = 5

(b) n = 120, k = 10

(c) n = 363, k = 15

(d) n = 1092, k = 25

Fig. 2. Detection rate varies with number of compromised nodes under different n =39, 120, 363, 1092, Interval = 2 Sec.

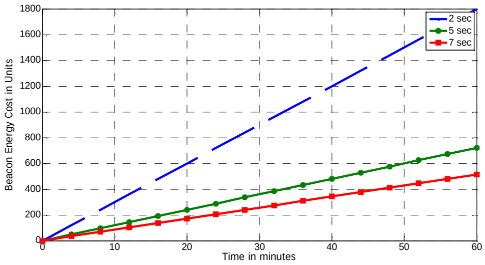
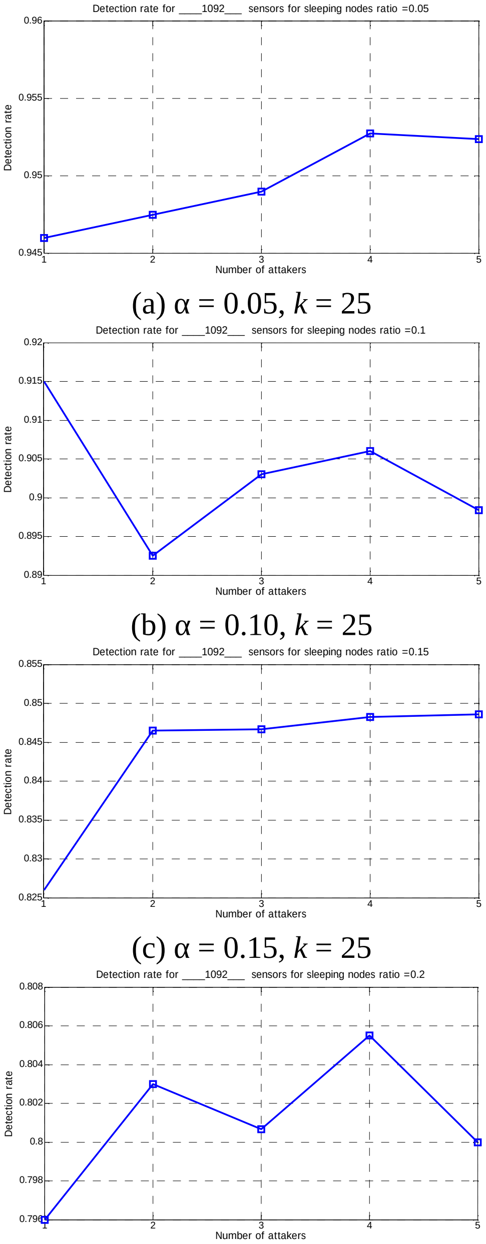


Fig.3. Beacon energy costs vary with the time period under different intervals



(a) α = 0.05, *k* = 25

(b) α = 0.10, *k* = 25

(c) α = 0.15, *k* = 25

(d) α = 0.20, *k* = 25

Fig. 4. Detection rate varies with n under different α = 0.05, 0.10, 0.15, 0.20, Interval = 2 Sec.

The detection rate is equal to the detected compromised sensor nodes over all compromised nodes.
In the proposed adversary model, we assume that an adversary can simultaneously compromise k sensor nodes, where $k<n$.
Thus, we first evaluate the detection rate under different parameters n, k and beacon interval and the results are shown in Figure 2. From Figure 2, we can see the detection rate does not increase linearly with k. When n = 363 or n = 1092, the detection rate reaches the maximum. Due to this observation, when the number of sensor nodes increase, we found that the proposed scheme has high resiliency against node compromise attack by collaborative work of attackers at the same time for large hierarchical WSN.
To improve the detection rate, we should choose a small interval. However, the energy costs used for sending/receiving beacon information will increase. Assume that sending/receiving one beacon information requires one unit energy; we compare the beacon energy costs under different intervals in Figure 3. Clearly, as shown in Figure 3, the smaller the interval, the higher the energy costs. Therefore, there is a tradeoff between the interval and the energy costs.
In the above simulation, similar to most previously reported work [4], we only consider that all sensor nodes are always active. However, in reality, in order to extend the network longevity, sensor nodes need to periodically enter into the sleep mode. In the sleep mode, a sensor node does not send or receive any messages from others. This will result in most power saving to the network. However, the sleep mode provides the attackers the best chance to compromise many legitimate sleeping sensor nodes while these nodes are not detected as compromised nodes. Assume that all n sensor nodes in a local area follow the same active/sleep schedule and sensor nodes within the groups are scheduling synchronization. For α the percentage of sleep nodes. At the same time, in each period, only α percent sensor nodes are in a sleep mode. With these settings, we run the above simulations again, where α has different values, interval 2 sec and number of sensor nodes n = 1092.
Figure 4 shows the detection rate in terms of different parameter α. From the figure, we can see that when α increases, the detection rate will decrease. Thus, this is another tradeoff between the detection rate and the network longevity when we choose the proper active/sleep schedule.

7. Conclusion:

In this paper, we proposed the overlapped groups-based compromised nodes detection scheme to early detect the node compromise attack in the first stage. Concretely, the simulation results showed that by building groups among neighboring sensor nodes in a local area, physical node compromise attack can be detected immediately. Also, the simulation results showed that the proposed detection scheme has high detection rate. This work is an initial work to form overlapped groups for detecting compromise attack at the first stage and we do not expect that the proposed scheme will solve all the problems in the node compromise nodes attack. Our future work will continue to build more overlapped groups to early detect the compromise nodes attack.

References:

[1] Mahmood Ali, Annette Böhm, and Magnus Jonsson, "Wireless Sensor Networks for Surveillance Applications – A Comparative Survey of MAC Protocols", 4th International Conference on Wireless and Mobile Communications, IEEE 2008.

[2] Tatiana Bokareva, Wen Hu, Salil Kanhere, Branko Ristic, Neil Gordon, Travis Bessell, Mark Rutten and Sanjay Jha, "Wireless Sensor Networks for Battlefield Surveillance", Proceedings of The Land Warfare Conference (LWC), October 2006.

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

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

[6] 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.

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

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

[9] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla, "Pioneer: verifying integrity and guaranteeing execution of code on legacy platforms," in SOSP, Oct. 2005.

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

[11] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao, "Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks", Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems, IEEE 2007.

[12] Xiaodong Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks", IEEE "GLOBECOM" 2009.

[13] Taejoon Park, and Kang G. Shin, "Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 4, No. 3, May/June 2005, IEEE 2005.

[14] Xiaojiang Du, “Detection of Compromised Sensor Nodes in Heterogeneous Sensor Networks”, IEEE "ICC" 2008.

Arvind Seshadri, Adrian Perrig, Leendert van Doorn, and Pradeep Khosla,
[15] “SWATT: SoftWare-based ATTestation for Embedded Devices”, In IEEE
Symposium on Security and Privacy (2004), IEEE Computer Society 2004.

[16] Tamer AbuHmed, Nandinbold Nyamaa, and DaeHun Nyang, “Software-Based Remote Code Attestation in Wireless Sensor Network”, IEEE "GLOBECOM" 2009.

[17] Jun-Won Ho, Matthew Wright, and Sajal K. Das, “ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Sensor Networks Using Sequential Analysis”, 2009 28th IEEE International Symposium on Reliable Distributed Systems, IEEE 2009.

[18] J. Deng, R. Han, and S. Mishra, “Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks”, In Proc. International Conference on Information Processing in Sensor Networks, pp. 292–300, ACM 2006.