Paper: ASAT-14-175-CM

14th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 14 – May 24 - 26, 2011, Email: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel: +(202) 24025292 –24036138, Fax: +(202) 22621908

Secure Network Recovery from Base Station Failure of Surveillance WSN in Hostile Environment

M.H. Megahed [*], Dimitrios Makrakis [†]

Abstract: Securing surveillance wireless sensor networks (WSNs) in hostile environments such as borders, perimeters and battlefields during Base Station (BS) failure is challenging. Surveillance WSNs are highly vulnerable to BS failure. The attackers can render the network useless by only destroying the BS as the needed efforts to destroy the BS is much less than that is needed to destroy the network. This attack scenario will give the attackers the best chance to compromise many legitimate nodes. Previous works have tackled BS failure by deploying a mobile BS or by using multiple BSs. Despite the best electronic countermeasures, intrusion tolerance and anti-traffic analysis strategies to protect the BSs, an adversary still can destroy them. This paper proposes a novel security architecture called Surveillance Security (SurvSec) for secure and reliable network recovery from single BS failure of surveillance WSN with single BS. SurvSec relies on a set of sensor nodes serve as Security Managers for management and storage of the security related data of all sensor nodes. SurvSec security architecture provides methodology for choosing and changing the security managers of the surveillance WSN. SurvSec has four components: (1) Sensor nodes serve as Security Managers, (2) Data Storage System, (3) Data Recovery System, (4) Security for the Data Storage System. Furthermore, both the frame format of the stored data is carefully built and the security threats are encoded to allow minimum overheads for SurvSec security architecture. In this paper, we provide detailed specifications of SurvSec security architecture along with its security system for secure and reliable network recovery from single BS failure. We evaluate our designed security architecture for reliable network recovery from BS failure. Our evaluation shows that the proposed new security architecture can meet all the desired specifications and our analysis shows that the provided Security Managers are capable of network recovery from BS failure.

Keywords: Security Manager; Wireless Sensor Network; Reliable; Network Recovery; Surveillance; Base Station; Failure, Secret Sharing.

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 will vary according to its mission which might be the presence of moving vehicles or target detection or other events

[*] School of Information Technology and Engineering, Electrical Engineering Department, University of Ottawa, Ottawa, Canada, mmega080@uottawa.ca .

[†] School of Information Technology and Engineering, Electrical Engineering Department, University of Ottawa, Ottawa, Canada, dimitris@site.uottawa.ca

where 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 first launch physical attacks against the BSs of surveillance WSN include jamming and destruction then they will compromise many legitimate nodes to destroy the deployed network security and to cover their unauthorized intrusions.

BS is a critical part of a WSN and an entire WSN can be rendered useless by taking down its BS. Indeed, it is crucial to protect a BS against both software-based and physical attacks. Several intrusion tolerant techniques have been developed to protect a BS against software-based remote attacks such as DoS attacks that flood the BS with packets, and remote spoofing of the BS to misdirect legitimate sensor data [3]. Software-based techniques cannot protect BS against physical attacks. Therefore, some works have been done to address the problem of protecting a BS against physical attacks through concealing its geographic location in the network [4].

Our focus in this work is to address single BS failure in single BS network. We consider a feasible attack towards single BS as single point of failure or even towards multiple BSs to render the whole WSN useless and after this attack collaborative work of attackers can compromise many legitimate nodes.

Also, previous works lack both the procedures to ensure network reliability and security during BS failure such as storing then sending reports concerning security threats against nodes to the new BS and the procedure to verify the trustworthiness of the deployed sensor nodes by the new BS otherwise a new WSN must be re-deployed which is a high cost and it needs time.

To the best of our knowledge, there has not been work done for securing the surveillance WSN during the time between the BS failure and the new mobile BS deployment which is the perfect time for attackers to compromise many nodes then destroy the security of the whole system. Also, there is not any work that describes how the new BS will verify the trustworthiness of the deployed WSN otherwise a new WSN must be deployed. Therefore, for mission critical applications such as surveillance WSN, if the BS fails, we propose to address this problem through employing our new designed security architecture of Surveillance Security (SurvSec) to detect the BS failure, monitor the network sensitive security issues to store security data in multiple replica, and send the stored data to the new BS after it is authenticated. Furthermore, BS failure shows the importance of reporting the monitored security threats to the new BS through securely storing this sensitive data then sending this data during the recovery process to the new BS.

These procedures will result in reliable recovery from such attack. BS failure can be alleviated such as work discussed in [5] by the use of multiple base stations deployed along the periphery of the field, and allowing each base station to act as a data sink, multiple BSs failure is an important performance metric which must be considered and it is a serious attack. Therefore, if the BS failed and the network nodes are not trusted by the new BS, the whole network must be redeployed. Re-deploying such mission critical large surveillance WSN shows the importance of SurvSec security architecture to efficiently recover from single BS failure and later on multiple BSs failure by updating the new BS with all the security information that is needed to trust the network nodes thus enabling to achieve reliable network recovery from BS failure.

In this paper, we present a novel recovery approach from BS failure that includes monitoring the network security issues to store the sensitive data, and send the stored data to the new BS after deployment to enable efficient recovery from BS failure while maintaining the operation of the network. Our motivation is the high probability of single BS failure as single point of failure to render the whole network ineffective. Our goal is to design new security architecture SurvSec for reliable network recovery from BS failure of surveillance WSN in hostile environment.

The **contributions** of this work can be summarized as:

The **first contribution** is the development of the new security architecture called Surveillance Security (SurvSec) for fast and reliable network recovery from BS failure of surveillance WSN with hierarchical data storage system.

The **second contribution** is the design of distributed security managers to enable distributed network security and distributed secure storage.

The **third contribution** is hierarchical data storage and data recovery system for the security data of the sensor nodes.

The **fourth contribution** is a proposed system to secure SurvSec security architecture.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 describes the assumptions, attacker model and network setup. Section 4 describes an overview of our security architecture SurvSec to recover from BS failure with its ingredients. Section 5 presents SurvSec data storage system and its analysis. Section 6 presents SurvSec data recovery system and its analysis. Section 7 presents SurvSec security for the stored data. Section 8 presents the simulation results. Finally, Section 9 concludes the paper.

2. Related Work

In this section, we present a brief overview of the related works such as some previous approaches taken towards enhancing BS security, fault tolerant models, and security protocols in wireless sensor networks.

Because the BS is a single point of failure and all the data is routed towards it, if it failed then the entire network can be disabled. Therefore, there are number of proposed strategies designed for securing the sensor network against the threats that can lead to the BS failure. These protocols are summarized as location concealing of BS through privacy algorithms [6], relocating the BS [7], using multiple mobile BSs [7], multipath routing to multiple BSs [3], intrusion tolerant software [8], and anti-traffic analysis strategies such as random fake paths to confuse the adversary and random areas of high communication activity [4].

Since BS and nodes are prone to failure due to energy depletion, hardware failure, communication link errors, software attacks and physical attacks, therefore, fault tolerance is one of the critical issues in WSNs. Fault tolerance is defined as the ability of the system to deliver a desired level of functionality in the presence of faults [9, 10].

All of the fault management protocols lack the procedures for secure and reliable network recovery from BS failure which are important issues for mission critical applications such as surveillance WSN in hostile environment.

There are different security protocols proposed and implemented for use with wireless sensor networks. In [11], Perrig et al. proposed Security Protocols for Sensor Networks, SPINS, a suite of security protocols optimized for sensor networks. It consists of two secure building blocks SNEP and μTESLA. In [12], Karlof et al. designed the replacement for the unfinished SNEP, known as TinySec..

All of the above security protocols lack the procedures for secure and reliable network recovery from BS failure which are important issues for mission critical applications such as surveillance WSN in hostile environment.

In this paper, we propose the first security architecture which is called surveillance security (SurvSec) for reliable network recovery from BS failure of surveillance WSN in hostile environment. More specifically, the architecture should allow two main steps. First step is the storage of security data to store the security data and secure the network instead of deploying a new network which is a high cost. The second step is the reliable recovery from BS failure by collecting the stored data to the new BS.

3. Network Assumptions, and Evaluation Metrics

3.1 Network Assumptions

We consider a hierarchical sensor network that is composed of large number of sensor nodes with unique ID and single base station placed in layers where one layer is defined as group of nodes connected to the upper sensor node. The nodes are arranged in clusters and it is assumed they have the ability to detect the compromised nodes. The nodes have Local Intrusion Detection System (LIDS) capable of detecting Cloning attack, Sybil attack and other attacks.

Meanwhile, some nodes continuously store the detected security threats and all other security data related to sensor nodes where these nodes are named security managers. Following the previous works on data storage in WSNs, there are several categories but two main approaches: Centralized data storage [13–16] which is suitable for streaming data applications, and Distributed data storage [17–21] which is suitable to provide information services to the authorized users such as soldiers in the battlefield. Other approaches are the centric data storage systems and those based on the collaborative work between sensor nodes to build the data storage infrastructure systems.

3.2 Evaluation Metrics

The evaluation metrics are the followings:

- Low communication overheads.
- Low storage overheads.
- Low recovery overheads.
- High network trustworthiness.
- Small distributed users’ table size.

4. Overview of SurvSec Security Architecture

In this section, we provide an overview of the SurvSec security architecture. The question arises what are the required procedures to store the security related data which will allow reliable network recovery from base station failure. Also, this section describes the functionalities of sensor nodes selected as security managers to employ the distributed security concept for the sensor network.

SurvSec has a security report and this report content is the security related data of sensor nodes which are: Node Index, and part of the reported attacks are: Node Compromise Attack, Revoked Node, Local Intrusion Detection (LID) Cloning Attack, LID Sybil Attack, LID Sinkhole Attack, LID Wormhole Attack, LID Selective Forwarding Attack, Node Outage, Awake Node, Sleep Node, Node Failure, Node Misbehavior, Selfish Node, Message Corruption, Routing Attacks, Denial-of-Service (DoS) Attacks, Security Level, Re-keying.

4.1 Security Managers Setup and Functions

In wireless sensor networks, all the security related information concerning the sensor nodes must be stored in a distributed manner in some sensor nodes which will be named security managers to allow the network to be able to verify the trustworthiness of the sensor nodes after security attacks and during all critical situations such as base station failure by retrieving the stored critical information of the security threats such as compromised node attack.

The security managers are responsible for the followings:

1- Storage and management of the security related data of sensor nodes.
2- Distribution and exchanging of the Shared Keys between sensor nodes for encryption.
3- Security managers have a very important feature to add to the security of the WSN which is its capability to stop data query from spreading to every sensor node by flooding messages. This feature provide the network with the ability to return data back to the sink from only the security managers where this data is concerning the security related data of all sensor nodes.

Security Managers Network Setup and the Methodology to Choose the Security Managers:

1- The base station has the network topology of all of the sensor nodes and their locations.
2- The base station divides the network into divisions of three layers as shown in Figure 1.
3- The base station assigns the first layer of the security managers as the sensor nodes cluster heads of the first layer sensor nodes. The security manager generates a group key between the security manager and its downstream sensor nodes.
4- The base station assigns the next layers of the security managers after three layers of the cluster heads and so on. The security manager generates a group key between the security managers and its downstream sensor nodes.
5- The base station changes the security managers from time to time according to the sensor nodes power and the life time of the network.

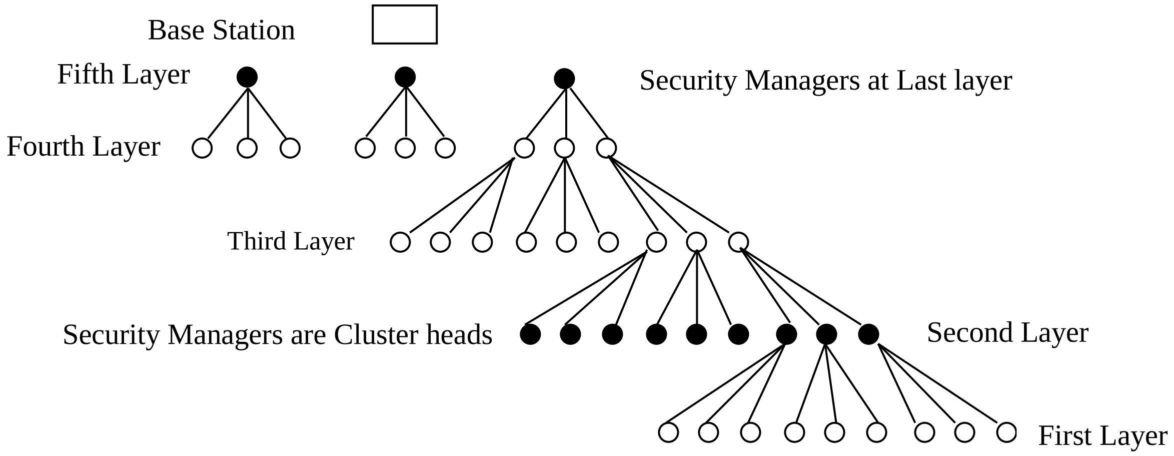

Figure 1 Security Managers Network Setup

4.2 Communications of Nodes in the Tree

We have two sensor nodes which are forwarding nodes and security managers’ nodes.

The security managers are chosen by the base station. If a security threat takes place at a sensor node, the sensor node will report the security threat to its security manager such as wormhole attack. Also, if a compromised node attack takes place at a senor node, the sensor node’s upper layer node in the hierarchical architecture will report this security threat to the security manager which is responsible for this sensor node.

4.3 SurvSec Components:

1. The main component of SurvSec is the hierarchical security managers which is vital to the implementation of the distributed security concept.
2. Second component is the data storage system with a proposed frame format for stored data.
3. Third component is the data recovery system.
4. Fourth component is the security for the data storage system.

5. SurvSec Data Storage System

In this section, we explain the stored data frame format and the security threats coding where we found that the base station failure is the worst attack scenario because the attacker can compromise many legitimate nodes and the new base station cannot verify the trustworthiness of the deployed sensor nodes of the network. The heart of our system is founded on the use of encoded attacks, stored data frame format and data recovery system to allow reliable network recovery from the base station failure of Surveillance WSNs. Our security system enables lightweight distributed data storage and recovery system using senor nodes called security managers.

5.1 SurvSec Nodes Indexing and Threats Coding

1. Nodes Indexing.

Each node has a unique node ID. The node ID is stored at the security manager unencrypted to be searched in case of incoming enquiries to investigate the sensor nodes security status.

2. Threats Coding.

We will build a table to encode each security threat into a determined bits code at that table which is loaded on each sensor node.

5.2 SurvSec Data Storage Frame Format

The stored data frame format is the following:

1- Count to present the attack number against the sensor node which is 7 bits to enable maximum attacks number of 128 attacks where the known attacks are less than 128 attacks. This count is 7 bits and it is sent by the node itself.
2- Time to present the time of the attack which is 17 bits to enable 5 bits for the hours, 6 bits for minutes and 6 bits for seconds. This time is 17 bits and it is added at the security managers.
3- Attack ID which is 6 bits to enable maximum attacks of 64 attacks. This attack ID is sent by the node itself.
4- Attacked node ID which is 10 bits to enable maximum number of 1024 nodes in each branch of sensor nodes. This node ID is sent by the node itself or by the monitored nodes.
5- Attacked node reputation which is 2 bits to enable 4 reputations levels which are good, medium, over medium and bad. It is added at the security managers.
6- Data replica number which is 6 bits to enable 64 data replicas within the security mangers. This data replica number is added at the security managers.
7- Stored record Data Integrity which is 32 bits to enable checking the integrity of the stored data records. This data integrity is added at the security managers.

The total stored data at the security manager of one monitored sensor node as one record for one attack is 80 bits and it will be increased by 80 bits for each different added attack. We expect to have one or two different attacks for each sensor node.

6. SurvSec Data Recovery System

This section describes our proposed recovery system where we found that we cannot use the erasure coding [22] to recover the error at the 6 bits of the attack ID because the number of used bits for error correction code will largely increase as the attacks increased. Also, the computations to generate and recover the errors of the encoded attacks will be high. Therefore, we proposed to use multiple replicas to ensure the correct query results when investigating the situation of a sensor node security status.

There must be at least three replicas of the stored data for data recovery where each data record specifying a sensor nodes security attacks is stored at least three times at three security managers to allow sending queries to two security managers at a time. The procedures for the stored data recovery system:

1- During the base station failure the sensor nodes send their security reports which include the attacks ID on the sensor nodes along with the data integrity for the stored data frame format of the security related data.
2- The security manager checks the data integrity of the sent data and if the security manager founds error in the process of verification for the data integrity, the security manager will send two queries to two security managers underneath to ensure the correct result of the attack ID for the reported senor node. If the two results are the same, therefore, there is no problem to accept the result. But, if the two results are different with polluted data integrity, the security manager will send a query to a third security manager to ensure the attack ID.
3- After the authentication process of the new deployed base station or the recovered base station, the last layer of the security managers will send the security related data of its downstream sensor nodes to the base station.
4- The base station checks the data integrity of the sent data and if the base station founds error in the process of verification for the data integrity, the base station will send two queries to two security managers underneath to ensure the correct result of the attack ID for the reported senor node. If the two results are the same, therefore, there is no problem to accept the result. But, if the two results are different with polluted data integrity, the base station will send a query to a third security manager to ensure the attack ID.

7. SurvSec Secure Data Storage System

In this section, we describe the dynamic secret sharing concept to generate our proposed distributed users table. This is done to generate a new dynamic secret sharing algorithm which is used to stop eavesdropping on the users that holds the secret shares with the security managers.

7.1 Secret Sharing:

This section describes Shamir secret sharing for which Shamir proposed an (m, n) Secret Sharing (SS) scheme [23] based on polynomial interpolation, in which m of n shares of a secret are required to reconstruct the secret [24].

Shamir's Secret Sharing: [25, 26]

The secret k is in Z_p (p is prime, and $p > n$). Each shareholder i is in the set P ($|P| = n$).

All mathematical operations are in the Finite Field Z_p.

To distribute k, select a polynomial $a(x)$ with degree ($m- 1$) and constant term k. Generate a share s_i for each i in P with $a(x)$: $s_i = k + \sum_{j=1}^{m-1} a_j\, i^j$ and s_i is also in Z_p.

To reconstruct k, retrieve m coordinate pairs (i, s_i) of all i in authorized subset B of P ($|B| = m$) and use the pairs in the Lagrange interpolation formula: $k = \sum_{i\in B} b_i\, s^i$, where

$b_i = \prod_{j\in B, j\neq i} \frac{j}{j-i}$.

7.2 Dynamic Secret Sharing:

Secret sharing scheme is a threshold scheme in that without enough shares the secret is information-theoretic secure. There exist many secret sharing schemes. One of them is Shamir's scheme based on polynomial interpolation. Other schemes are dynamic secret sharing depends on changing the polynomial and changing the users.

1. Dynamic Secret Sharing by Dynamic Polynomials:

The dynamic polynomial can depend on changing the shared secrets. This is done to eliminate the weaknesses of the secret sharing such as eavesdropping to know the shares holders. In 1994, He and Dawson [27] proposed a multistage secret sharing scheme based on the one-way function. By applying successive one-way hash functions, the He-Dawson scheme realized the notion of multi-secret sharing. Yet, in 2007, Geng et al. [28] pointed out that the He-Dawson scheme was actually the one-time-use scheme [29] and further proposed a new multi-secret sharing scheme with multi-policy.

2. Dynamic Secret Sharing by Adding New Users:

Dynamic secret sharing can be done by adding new users which is known as multi-level secret sharing. In Multi-Level Secret Sharing, shares have distinct weight (impact) in the secret construction. That is, secret construction requires less number of weightier shares but more number of lighter shares. The Simmons [30] introduced the disjunctive multi-level access structure. Tassa [31] introduced the conjunctive multi-level access structure. M. Belenkiy [32] recently presents a disjunctive multi-level secret sharing scheme. That is the first polynomial-time solution that allows the dealer to add new users dynamically and by far the most efficient.

7.3 Proposed Distributed Users Table:

In this section, we describe our designed dynamic secret sharing which includes dynamic users by changing of the shared users in the distributed users tables. Each SM shares its downstream sensor nodes multiple shares of secrets to build the used key for the encryption process which is carried out on the SM to securely store the security related data of sensor nodes.

Adding distributed users table to secret sharing will allow the addition and the change of users to enable dynamic users for the secret sharing and this is done to stop eavesdropping during encryption of security related data.

Our dynamic secret sharing includes reconfigurable distributed users tables to change the shared users after only two hops.

The total number of nodes around the SM after two hops, which is our bounded limits for multiple hops around the SM, represents the total nodes space which shares the SM the key space that is used to encrypt the stored data of security related information.

Therefore, we will have a large group of nodes which can share the SM the shared secrets with the ability to join new nodes and change other nodes. Furthermore, the members of the distributed users table must be able to deliver the request of the SM to its destination and must be able to deliver the required shared secret from the destination to the SM.

We need to update the distributed users table from time to time depending on the detected compromised nodes. This is done to ensure that there is no compromised sensor node that holds a secret with the security manager sensor node.

The process to build the distributed users table:

1- The BS assigns the security managers and its downstream sensor nodes.
2- The SMs discover its downstream sensor nodes.
3- Each SM shares a group key with its downstream sensor nodes.
4- Each SM builds the distributed users table from knowing its downstream sensor nodes.
5- SMs communicate with its shared nodes to share secrets with the SMs in only two hops since the security managers are each three layers and each sensor node needs to store only one distributed users table to lower storage overheads.
6- Each sensor node will store only one distributed users table which is shared with its security manager.

7- The distributed users table has a significant property to add to the system that it allows the dynamic change of the table through reconfiguration of the table where distributed users tables are reconfigurable to change the users and this is done to allow dynamic security.

The following table is the overall distributed users table assuming there are five sensor nodes downstream the security managers:

Table 1 Overall Distributed Users Table

Index	Count & Reconfigured Count	First hop Node	Second hop Node	Destination
1	1	1	0X 6 - A	0X 06,0B,00,16,00
2	2	2	0X B - F	0X 07,0C,12,00,00
3	3	3	0X 11 - 15	0X 08,0D,00,18,00
4	4	4	0X 16 – 1A	0X 09,0E,00,00,1E
5	5	5	0X 1B – 1F	0X 0A,00,15,1A,00

1- We assume that each security manager has 5 downstream nodes and we assume we need only 3 shares to reconstruct the secret information which is the key.

2- The count field represents the counted attacks to the sensor nodes downstream the SM. This field is increased by 5 after it is used. Using the counted attack will result in definite sensor nodes at the destination to share the secret with the SM.

3- The second field is the first hop sensor node.

4- The third field is the second hop sensor nodes.

5- The fourth field is the destination sensor nodes and then first destination is set to hexadecimal value of 06, the second destination is set to hexadecimal value of 0B, the third destination doesn’t share any secrets with the SM, the fourth destination is set to hexadecimal value of 16, and the fifth destination doesn’t share any secrets with the security manager.

The following table is the distributed users table at the security manager. It explains the data to the first hop sensor node to deliver requests from security manager to first hop sensor node and to return requests from the first hop sensor node to the security manager:

Table 2 Distributed Users Table at the Security Managers Sensor Nodes

Index	Count & Reconfigured Count	Destination Nodes	Path
1	1	0X 06,0B,00,16,00	1-6, 2-B, 3-0, 4-16, 5-0
2	2	0X 07,0C,12,00,00	1-7, 2-C, 3-12, 4-0, 5-0
3	3	0X 08,0D,00,18,00	1-8, 2-D, 3-0, 4-18, 5-0
4	4	0X 09,0E,00,00,1E	1-9, 2-E, 3-0, 4-0, 5-1E
5	5	0X 0A,00,15,1A,00	1-A, 2-0, 3-15, 4-1A, 5-0

1- We count the sensor nodes downstream the SM with 2 hops where the SM has 5 downstream sensor nodes and each node has 5 downstream sensor nodes with total of 30 sensor nodes downstream the SM.

2- The path column is not used because it is the explanation of the destination column where the first location 0X06 means the destination is the sensor node number 0X6 from the first node at the first hop from the security manager.

3- Also, 0X0B means the destination is the sensor node number 0XB through the second node at the first hop from the security manager.

4- Also, 00 means that there is no destination sensor node through the third and fifth node at the first hop from the security manager. This is done because there are only three sensor nodes that shares secrets with the security manager.
5- Also, 0X16 means the destination is the sensor node number 0X16 through the fourth node at the first hop from the security manager.
6- Each node at two hops from the SM takes unique number from 0X00 to 0XFF hexadecimal values.
7- The size of the table at the security manager is 240 bits from 40 bits at each field in the third column where there are five sensor nodes each has 8 bits, and the reconfigured count is 8 bits. Therefore, we have 40 bits multiplied by 5 records and 8 bits multiplied by 5 records with total of 240 bits data.

The following table is the distributed users table at the first hop sensor nodes. It explains the data to the second hop sensor node to deliver requests from the first hop sensor nodes to the second hop sensor node and return the requests to the security manager:

Table 3 Distributed Users Table at the First Hop Sensor Nodes

Index	Node at first hop	Path at second hop
1	1	0X 6 - A
2	2	0X B - F
3	3	0X 11 - 15
4	4	0X 16 – 1A
5	5	0X 1B – 1F

The first raw is stored at the first sensor node and the second raw is stored at the second sensor node and so on. The table size is 40 bits at each sensor node where we have five users each has 8 bits.

The path column at second hop first locates where the destination is then it locates the sensor node to that destination. Also, sensor node at the first hop which is number one takes only raw number one and so on.

The following table is the distributed users table at the second hop sensor nodes. It explains the data to return requests from second hop sensor node to the first hop table:

Table 4 Distributed Users Table at the Second Hop Sensor Nodes

Index	Node at first hop	Path at second hop
1	1	0X 6 - A
2	2	0X B - F
3	3	0X 11 - 15
4	4	0X 16 – 1A
5	5	0X 1B – 1F

The first raw is stored at the first sensor node and the second raw is stored at the second sensor node and so on. The table size is 40 bits at each sensor node where we have five users each has 8 bits.

The path column of second hop only locates where the destination is from second hop sensor node to first hop sensor node. Also, sensor node at the second hop which is number one takes only raw number one and so on.

The main contributions for our proposed dynamic secret sharing algorithm with distributed users table are explained in this section as we proposed a novel idea of distributed users table based on the concept of dynamic secret sharing. Our proposed security scheme has the following properties:

1- It provides dynamic secret sharing with adding and changing of multiple users;
2- It can limit the damage from compromised sensor nodes since the compromised node can be easily revoked from the distributed users table;
3- It preserves small size for distributed users table but with high search space for the attacker to decrypt the secure stored data;
4- It is scalable to large sensor networks due to its lightweight computation and easy key management.
5- The stored secure data contains the users used for the secret sharing.

8. Simulation Results and Performance Analysis

We built an analytical model for the proposed design and we implemented a simulator in MATLAB that can scale to thousands of nodes. In this simulator, sensors can send and receive data from each other's. This data is the security related data regarding the security reports of sensor nodes. 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 10.000 sensor nodes.

The followings are the built models for simulation:

1- Network setup model for the security managers.
2- Attacker model.
3- Changing of security managers' model.
4- Data storage model.
5- Data recovery model.
6- Security model to secure the stored data using distributed users table
7- Update / Delete security related data model.
8- Network trustworthiness model.

8.1 Metrics:

The following metrics are considered.

1- Communications overheads: it is defined as the number of queries sent form the sensor node to the security manager (SM) result from number of attacks then from the SM to other SMs until the last SM at the last layer of sensor nodes near the base station (BS). We need SurvSec to have minimum communications overheads. Figure 2 shows that the communications overheads increase as the number of attacks increase.

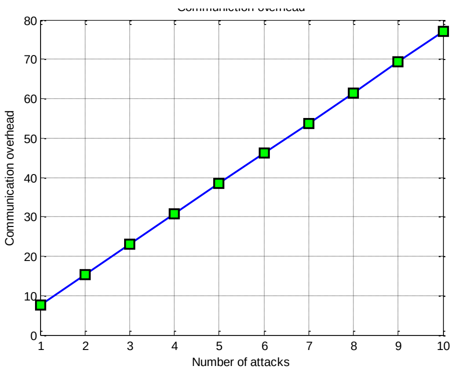

Figure 2 Communications Overheads

We assume eight layers sensor network and each attack is at the first layer which will result in eight communication overheads at all layers of the sensor network as shown in Figure 2. When an attack occurs at the first layer sensor nodes as shown in Figure 1 the attacked sensor node will send to its security manager with one communication overhead and so on until the BS with total of 8 communications overheads.

Communication overheads=K X n.

where K is (number of layers – the layer of the attack + 1) and n is (number of attacks)

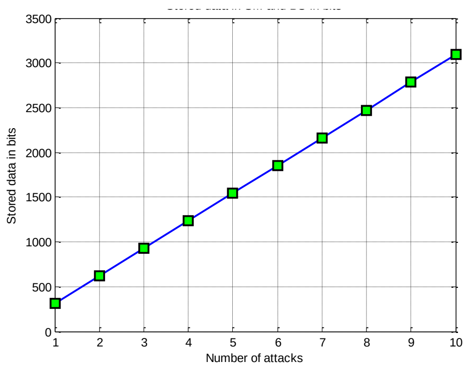

Figure 3 Storage Overheads

2- Storage overheads: it is defined as the total stored data at the entire security managers' plus the base station which results from number of attacks. Figure 3 shows that the storage overheads increase as the number of attacks increase. We assume eight layers sensor network and each attack is at the first layer which will result in storing the data at three security managers and BS with total of 320 bits storage overheads where one attack store 80 bits of security data as shown in Figure 3.

Data storage overheads = 80 X K X (n+1),

where K is (number of attacks) and n is the number of security managers storing one copy of the security related data and we add one because the BS also stores the security related data.

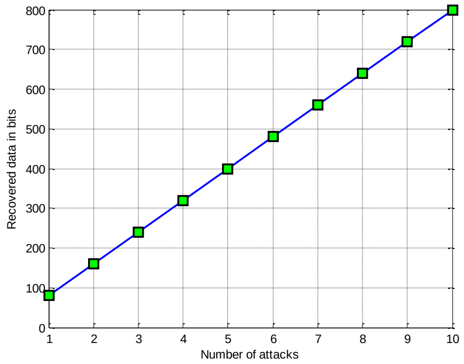

Figure 4 Recovered Data to Base Station

3- Recovered data overheads: it is defined as the needed data to recover from the attacks at the sensor nodes after the deployment of the new base station. Figure 4 shows that the recovered data overheads increase as the number of attacks increase. We assume eight layers sensor network and one attack can be recovered from 80 bits stored data at the last layer of the security managers near the base station as shown in Figure 1. The recovered data overheads can be shown in Figure 4.

Data recovery overheads = 80 X n,

where n is (number of attacks),

8.2 Efficiency:

We now assess the performance of the proposed SurvSec security architecture in terms of the network trustworthiness after the deployment of the new base station and the distributed users' table size. Therefore, first we will analyze the network trustworthiness for our proposed security architecture then second we will analyze the distributed users' table size versus the number of nodes in each layer.

1- Network Trustworthiness:

The attacked security managers are critical to the efficiency of SurvSec. Generally speaking, the more attacked security managers the less network trustworthiness. Figure 5 shows the network trustworthiness without any attacks at the security managers while Figure 6 shows an increasing rate of

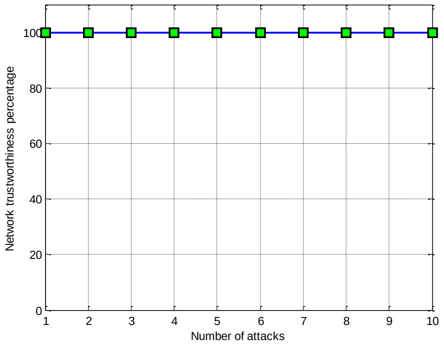

Figure 5 Network Trustworthiness without Attacked Security Managers

attacking the security managers which will result in decreasing the network trustworthiness.

The network trustworthiness is 100% in case there is no attacked security manager and this can be shown in Figure 5. Then this network trustworthiness ratio decreases when the security managers attacked because the security managers as security data senders cannot send their security reports and this can be shown in Figure 6.

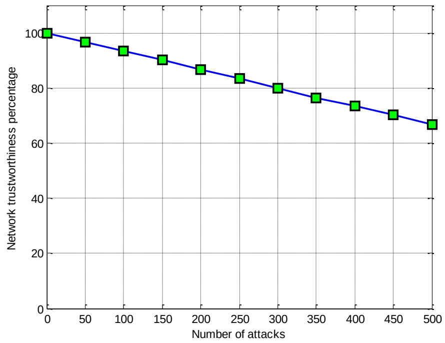

Figure 6 Network Trustworthiness with Attacked Security Managers

2- Distributed Users' Table Size:

The distributed users' table is critical part for SurvSec Security Architecture to enable delivering the requests of the SM to its destination for encryption and delivering the required shared secret from the destination to the SM. Figure 7 shows the distributed users' table size versus the number of nodes in each layer where the size increases as the number of sensor nodes in each layer increases. From Table 2, for three sensor nodes in each layer, the distributed users table size is 160 bits where we have five records each has count of 8 bits with total of 40 bits and 24 bits at each field in the third column where there are three sensor nodes each has 8 bits with total of 24 bits multiplied by 5 records added to 40 with total of 160 bits.

From Table 2, for four sensor nodes in each layer, the distributed users table size is 200 bits where we have five records each has count of 8 bits with total of 40 bits and 32 bits at each field in the third column where there are four sensor nodes each has 8 bits with total of 32 bits multiplied by 5 records added to 40 with total of 200 bits. We found that the distributed users' table size increases with 40 bits for adding one sensor node at each layer.

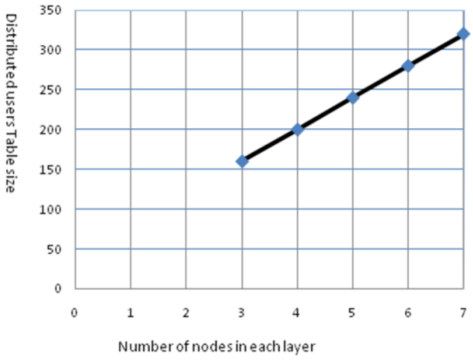

Figure 7 Distributed Users Table Size

9. Conclusion

In this paper, we proposed the first security architecture to achieve secure and reliable network recovery from base station failure. Concretely, we proposed a secure and reliable network recovery from base station failure of surveillance wireless sensor network in hostile environment to improve the security data survival capability in presence of base station failure. We further enhance such scheme by employing distributed security managers and distributed users' table. Our scheme is resilient to base station failure through our designed data storage and recovery systems.

The performance analysis and the simulation results of our proposed hierarchical secure data storage and recovery system provide the WSN with high confidence for secure and reliable network recovery from the base station failure of surveillance WSN in hostile environment.

10. References

[1] Mahmood Ali, Annette Böhm, and Magnus Jonsson, “Wireless Sensor Networks for Surveillance Applications – A Comparative Survey of MAC Protocols”, The Fourth International Conference on Wireless and Mobile Communications, **IEEE** 2008.Auth1,

[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] Jing Deng, Richard Han, and Shivakant Mishra, “Intrusion Tolerance and Anti-Traffic Analysis Strategies For Wireless Sensor Networks”, Proceedings of the International Conference on Dependable Systems and Networks DSN 2004, **IEEE** 2004.

[4] Jing Deng, Richard Han, and Shivakant Mishra, “Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks”, Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks SECURECOMM 2005, Pp 113 – 126, **IEEE** 2005.

[5] Shashidhar Rao Gandham, Milind Dawande, Ravi Prakash and S. Venkatesan, “Energy Efficient Schemes for Wireless Sensor Networks with Multiple Mobile Base Stations”, GLOBECOM 2003, **IEEE** 2003.

[6] Xinfeng Li, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, and Ming Gu, “Enhanced Location Privacy Protection of Base Station in Wireless Sensor Networks”, 2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks, **IEEE** 2009.

[7] Eylem Ekici, Yaoyao Gu, and Doruk Bozdag, “Mobility-Based Communication in Wireless Sensor Networks”, IEEE Communications Magazine, July 2006, **IEEE** 2006.

[8] Jing Deng, Richard Han, and Shivakant Mishra, “INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks”, Computer Communications, Volume 29, Issue 2, January 2006, Pp. 216-230, **ACM** 2006.

[9] Hai Liu, Amiya Nayak, and Ivan Stojmenovi, “Fault-Tolerant Algorithms/Protocols in Wireless Sensor Networks”, Guide to Wireless Sensor Networks, Computer Communications, **Springer** 2009.

[10] S. Chessa, and P. Maestrini, “Fault Recovery Mechanism in Single-Hop Sensor Networks”, Computer Communications 28 (2005) 1877–1886, **Elsevier** 2005.

[11] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, “SPINS: Security Protocols for Sensor Networks”, Wireless Networks, Volume 8, Issue 5, September 2002, Pp. 521-534, **ACM** 2002.

[12] Karlof, C., Sastry, N., and Wagner, ‘TinySec: A Link Layer Security Architecture for Wireless Sensor Networks’, Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 03 – 05 November 2004, Pp. 162 – 175, **ACM** 2004.

[13] Bonnet, J. Gehrke, and P. Seshadri, “Towards Sensor Database Systems”, In the Proceedings of the Second International Conference on Mobile Data Management, pp. 3–14, **Springer** 2001.

[14] S. Madden, M. Franklin, J. Hellerstein, and W. Hong. Tag, “A Tiny Aggregation Service for Ad-Hoc Sensor Networks”, In the Proceedings of the 5th Symposium on Operating Systems Design and Implementation OSDI, **ACM** 2002.

[15] Y. Yao and J. Gehrke, “Query Processing in Sensor Networks”, In the Proceedings of Conference of Innovative Data Systems Research CIDR, **IEEE** 2004.

[16] M. Sharaf, J. Beaver, A. Labrinidis, and P. Chrysanthis, “TiNA: A scheme for Temporal Coherency-aware in-Network Aggregation”, In Proceedings of the 3rd ACM International Workshop on Data Engineering for Wireless and Mobile Access MobiDE, **ACM** 2003.

[17] Abhishek Parakh and Subhash Kak, “A Distributed Data Storage Scheme for Sensor Networks”, MobiSec 2009.

[18] Norbert Siegmund, Marko Rosenmuller, Guido Moritz, Gunter Saake, and Dirk Timmermann, “Towards Robust Data Storage in Wireless Sensor Networks”, the IETE Journal 2009.

[19] R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Data Survival in Unattended Sensor Networks”, In 6th Annual International Conference on Pervasive Computing and Communications (PerCom ’08), **IEEE** 2008.

[20] N. Subramanian, C. Yang, and W. Zhang, “Securing Distributed Data Storage and Retrieval in Sensor Networks”, In International Conference on Pervasive and Mobile Computing (PerCom 2007), **Elsevier** 2007.

[21] Wei Ren, Yi Ren, and Hui Zhang, “HybridS: A Scheme for Secure Distributed Data Storage in WSNs”, **IEEE** 2008.

[22] S.Reed and G.Solomon, “Polynomial Codes over Certain Finite”, IEEE 1960.

[23] R. Rivest, and Adi Shamir, “How to Share a Secret”, **ACM** 1979.

[24] Qian Wang, Kui Ren, Wenjing Lou, and Yanchao Zhang, “Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance”, INFOCOM, **IEEE** 2009.

[25] Wei Ren, Yi Ren, and Hui Zhang, “HybridS: A Scheme for Secure Distributed Data Storage in WSNs”, International Conference on Embedded and Ubiquitous Computing, **IEEE** 2008.

[26] Wei Ren, Junge Zhao, and Yi Ren, “MSS: A Multi-level Data Placement Scheme for Data Survival in Wireless Sensor Networks”, **IEEE** 2009.

[27] J. He, and E. Dawson, “Multistage Secret Sharing Based on One-Way Function”, Electronics Letters, 30 (19) (1994) 1591-1592.

[28] Y.J. Geng, X.H. Fan, and F. Hong, “A New Multi-secret Sharing Scheme with Multi-policy”, The 9th International Conference on Advanced Communication Technology, Vol. 3, 2007, pp. 1515-1517.

[29] W.A. Jackson, K. M. Martin, and C. M. O’Keefe, “On Sharing Many Secrets”, Advances in Cryptology − ASIACRYPT’94, **Springer**-Verlag, 1994, pp.42-54.

[30] G. J. Simmons, “How to (Really) Share a Secret,” in the Proceedings of CRYPTO88, 1988, pp. 390–448.

[31] T. Tassa, “Hierarchical Threshold Secret Sharing,” in the Proceedings of TCC04, 2004.

[32] M. Belenkiy, “Disjunctive Mmulti-level Secret Sharing,” Cryptology ePrint Archive, Report 2008/018, 2008, http://eprint.iacr.org/.