Analytical Analysis of a Cluster Controlled Mobility Scheme for Data Security and Reliability in UWSNs

Amir S. Elsafrawey1, Emad S. Hassan2, and Moawad I. Dessouky3

1, 2, 3 Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt.

1elsafrawey@yahoo.com, 2emad.hassan@el-eng.menofia.edu.eg, 3dr_moawad@yahoo.com.

Abstract - This paper investigates the security and data reliability in Unattended Wireless Sensor Networks (UWSNs). We deduce an analytical model for Self-Healing scheme based on Cluster Controlled Mobility (SH-CCM) for UWSNs. The SH-CCM is based on mobility inside a cluster of sick sensor beside the hybrid cooperation from both reactive and proactive peers to enhance self-healing probability. The analytical analysis of SH-CCM will ensure that both mobility and hybrid cooperation from both reactive and proactive peers within the cluster of sick sensor will enhance the Cooperation, Self-Healing, data security and reliability. Therefore, the proposed SH-CCM scheme will help the sick sensor to self-heal and restore its backward secrecy faster and better than the schemes without controlled mobility. A set of Analytical results are carried out to demonstrate the effectiveness of the proposed SH-CCM scheme in the presence of an Adversary (ADV). The obtained results ensure that the proposed scheme has a better performance; it archives a probability of BSe to be compromised of 0.04 while CHSHRD [1] is 0.065.

Keywords – Unattended Wireless Sensor Network, Sensor Mobility, Sensor Cooperation, Mobile Adversary, Self-Healing.

I. INTRODUCTION

Unattended Wireless Sensor Network (UWSN) [1-3] is a class of Wireless Sensor Network (WSN), they are applicable to a wide range of applications [4-6]. UWSNs contain large number of sensors to sense data in a hostile environment. Sink visits the network every T time, so there is no real-time reporting of sensed data, thus exposes the data to adversary (ADV) threats. ADV can compromise sensors, it can learn sensor’s secret keys, encryption and decryption functions. It is desired to reduce the risk of compromising, there are many existing solutions for this challenge. The first solution depends on the presence of an online trusted sink, the second depends on the availability of a True Random Number Generator (TRNG) built in each sensor; both solutions are not suitable for large scale networks [2, 7]. The third one depends on the availability of a tamper-resistance on each sensor [8], but it is not suitable for low-cost sensor product. The forth solution depends on the cooperation principal; sensor cooperation has been shown to be an effective solution in UWSNs [11]. Finally, the mobility can be used to help and improve the chance of self-healing [9]. Sensor mobility enables a new set of possibilities in sensor networks; it is the complementary solution of the leakage of health peers. The change in sensor location can be used to mitigate/solve many of the design challenges or network problems [10-13]. There are different types of mobility models used in networks simulations [14].

Some previous work has considered the aforementioned challenges as follows. Pietro et al. [15] explored intrusion resilience in mobile UWSNs in the presence of mobile adversary. The authors in [16] defined a new security metrics to evaluate intrusion resilience protocols for mobile sensor networks. In [17] the authors leveraged sensor mobility and collaboration in mobile UWSNs in order to obtain intrusion-resilience with low overhead; they assumed a spherical deployment surface and a stationary adversary. Iida et al. [18] improved the schemes proposed in [15-17] from the viewpoint of both security and efficiency. The importance of mobility to improve the network coverage has been studied in [19]. Wang et al. in [20] explored the motion capability to relocate sensors to deal with sensor failure or respond to new events. In [21] Dutta et al. proposed a new self-healing key distribution scheme with revocation capability that requires constant storage of personal keys for each user but this scheme requires sink presence which unsuitable for UWSNs. In [22] the authors used the sensor mobility to improve the sensor capture detection.

In this paper, we present analytical analysis of the SH-CCM scheme [9] for UWSNs which uses the sensors mobility within a cluster of sick sensors beside the cooperation between both types of peers, so an infusion between sensors can occur which increase the chance of finding health neighbours. Hence it enhances both data security and reliability. Similar to [9], we define mobility model called Random Jump Controlled Mobility (RJCM) model which
supports controlled mobility and only applied for some of the network sensors. The choice of these sensor will based on the idea that sensor tampering will require that the sensor to be removed from the network for a non-negligible amount of time [23]. Therefore, we can use a sensor capturing detection algorithm to distinguish compromised sensor from health sensors [22].

The rest of this paper is organized as follows. Section 2 presents the network model and system assumptions. The proposed scheme analytical analysis is explained in Section 3. Then, Section 4 presents the theoretical and numerical results and discussion. Section 5 gives the concluding remarks.

II. NETWORK MODEL AND ASSUMPTIONS

A. The Network Model

We assume a homogenous static UWSN consists of N sensors uniformly distributed. UWSN can be formulated as an undirected graph G(N, E) [24]. Each sensor has a unique ID and is capable of sensing a circular area of radius called the Sensor Range (SR). Each sensor has neighbors set NR. The basic security mechanism is the pairwise keys to secure sensor-to-sensor and sink-to-sensor communication [25-26]. All sensors are identical in terms of radio interface, limited power, storage space, computational capability and ability to move. During initialization, each sensor performs one-way cryptographic hashing and symmetric key encryption based on a Pseudo-Random Number Generator (PRNG) initialized with a unique secret seed shared with the sink. We assumed a roving data sink to be a trusted party that cannot be compromised [27]. It visits the network for backing up the data stored, clearing the memories of all sensors, and update cryptographic material of each sensor. The sink could be an airplane or an army troop approaching the network. The time interval between two successive visits of the sink T is divided into rounds and all sensor clocks are loosely synchronized [28].

B. The Adversary Model

Adversaries (ADVs) can be classified into different classifications [25-30]. In this paper, we assume a proactive-centralized-mobile-not focused-logically ADV that trying to compromise number of sensors logically within its range. The ADV can subverts the entire network as it moves between sets of compromised sensors before the next visit of the sink. Our adversary model resembles that in [2-3] and has the following exclusive capabilities:

- ADV appears randomly once each round within the network.
- Range, and network density; will control the number of compromised sensors.
- Due to random appearance, ADV is unpredictable and untraceable.

C. Compromising Problem

Since the UWSN deployed in a hostile environment, and due to the sink absence most of the time, this cause that the sensors are easy target to be compromised by an ADV. During the sink absence, ADV occupies sensor at round r1 and releases it at round r2 (r2 > r1), the sensors are compromised the stored data are exposed to attack, the time can be partitioned into three categories: (1) before r1, (2) between r1 and r2, and (3) after r2. Nothing about secrecy of data that falls into category (2) since the ADV can learn and hold all keys k//r ∈ [r1, r2] and drive all future keys k//r' (r' > r2). The challenges become twofold: first, for category (1), the pre-compromise data must not be revealed if a sensor is compromised, and it is called Forward Secrecy FSe. Second, for category (3), the challenge is how to guarantee that the post-compromised data to be not exposed; this is called Backward Secrecy BSe.

D. Data Secrecy

Data secrecy can be guaranteed or at least probabilistic guaranteed for categories (1) and (3). For category (1); the FSe of sensor can be achieved by a periodic updating of its zero round secret key k/0 using one way collision resistant hash function H() and PRNG of this sensor to produce the current round secret key k// from the previous one k//−1. The benefit of hash function is that it cannot work in the reverse direction. Hence the ADV drive all future keys k//r' (r' > r2), therefore the BSe is not guaranteed and the data reliability is difficult to achieve. So, the encryption can only guarantee ESe but it isn’t enough to achieve BSe. We will interest in the confidentiality and reliability of data collected in category (3).

III. THE PROPOSED ANALYTICAL MODEL

Before starting with the Analytical analysis of the SH-CCM scheme, there are initial steps such as network initialization, encrypted data generation, data parts generation, node selection protocol, and data distribution which are explained in details in [1,9].

The analytical model will follow the model presented in [1], but with mobility synthesis, it will be applied at both network level and cluster level. Sick sensor can regain its BSe and protect data storage by explicitly implore for cooperation with Repeer and/or Propeer in conjunction with the mobility scheme as will be shown. First, let us define the following notations and symbols as shown in Table 3.
During the first round and after the ADV leaving, the self-healing process will start at network level as the following: Propeers will initialize and offer their help for a sick $s$, so for $k$ revoked sensors from the network, the probability to select $t_1$ of Propeers will be:

$$P_{pro.peers} = \frac{t_1}{n-k}$$  \hspace{1cm} (1)

The sick $s$ will fail to self-heal for two events ($A_p, B_p$). Event $A_p$ represents the probability that there is no any Propeers:

$$P(A_p) = 1 - P_{pro.peers} = 1 - \frac{t_1}{n-k}$$ \hspace{1cm} (2)

Event $B_p$ represents the probability that the ADV intercepts the contribution of Propeers:

$$P(B_p) = P_{pro.peers} \cdot p = \frac{t_1}{n-k} \cdot p$$ \hspace{1cm} (3)

The probability that $s$ is still sick at round $r + 1$ is:

$$p_{sick, Pro}^{r,r+1} = (P(A_p) + P(B_p))^{Hs^r}$$ \hspace{1cm} (4)

$$Hs^r = n \cdot p_{health}^{r-1} - 2 \cdot k$$ \hspace{1cm} (5)

$$p_{sick, Pro}^{r,r+1} = (1 - \frac{t_1}{n-k} + \frac{t_1}{n-k} \cdot p)^{n \cdot p_{health}^{r-1} - 2 \cdot k} = (1 - t_1 \cdot \frac{1-p}{n-k})^{n \cdot p_{health}^{r-1} - 2 \cdot k}$$  \hspace{1cm} (6)

$$p_{occu, Pro}^{r} = (p_{occu, Pro}^{r-1} + p_{sick, Pro}^{r-1}) \cdot p_{sick, Pro}^{r,r+1}$$ \hspace{1cm} (7)

$$p_{sick, Pro}^{r,r+1} = (p_{occu, Pro}^{r-1} + p_{sick, Pro}^{r-1}) \cdot \frac{k}{n \cdot p_{health}^{r-1} + k}$$ \hspace{1cm} (8)

$$p_{occu, Pro}^{r} = \frac{k}{n \cdot p_{health}^{r-1} + k}$$ \hspace{1cm} (9)

The probability of $s$ is still compromised for the next rounds will be:

$$p_{comp, Pro}^{r} = p_{sick, Pro}^{r} + p_{occu, Pro}^{r}$$ \hspace{1cm} (10)

$$p_{comp, Pro}^{r} = (p_{occu, Pro}^{r-1} + p_{sick, Pro}^{r-1}) \cdot (1 - t_1 \cdot \frac{1-p}{n-k})^{n \cdot p_{health}^{r-1} - 2 \cdot k} + \frac{k}{n \cdot p_{health}^{r-1} + k}$$ \hspace{1cm} (11)

Repeers are asked for help by a sick $s$, the sick $s$ will fail to self-heal for two events ($A_R, B_R$). So for $k$ revoked sensors from the network, Event ($A_R$); the probability is that there are no Repeers to select $t_2$ from them will be:

$$P(A_R) = \frac{\left(\frac{n \cdot p_{comp}^{r}}{t_2}\right)}{\left(\frac{n-k}{t_2}\right)}$$ \hspace{1cm} (11)
Event \((B_R)\), represents the probability that the ADV intercepted the selected \(t_2\) peers will be:

\[
P(B_R) = \sum_{i=1}^{t_2} p_i \cdot \left( \frac{n(1-p_{\text{comp}}^i)^{2k}}{t_2} \right) \left( \frac{n_p^r}{t_2-i} \right)
\]

\((12)\)

The sum of the two events probabilities give the probability that the sick \(s_i\) will remain sick for the next round:

\[
p_{\text{sick.Re}} = p_{\text{_occu.Re}} + p_{\text{sick.Re}} = \frac{k}{n_p \text{health} + k}
\]

\((13)\)

The probability of \(s_i\) being sick will be:

\[
p_{\text{sick.Re}} = (p_{\text{occu.Re}} + p_{\text{sick.Re}}) p_{\text{sick.Re}}
\]

\((14)\)

The probability of \(s_i\) being occupied will be:

\[
p_{\text{occu.Re}} = \frac{k}{n_p \text{health} + k}
\]

\((15)\)

The probability of \(s_i\) being compromised at round \(r\) and still compromised for the next rounds will be:

\[
p_{\text{comp.Re}} = p_{\text{comp.Re}} + p_{\text{occu.Re}}
\]

\((16)\)

\[
p_{\text{comp.Re}} = (p_{\text{occu.Re}} + p_{\text{sick.Re}}) p_{\text{comp.Re}} + \frac{k}{n_p \text{health} + k}
\]

\((17)\)

\[
p_{\text{comp.Re}} = (p_{\text{occu.Re}} + p_{\text{sick.Re}}) \left( \frac{n_p^r}{t_2} \right) \left( \frac{n_p^r}{t_2-i} \right) + \frac{k}{n_p \text{health} + k}
\]

\((18)\)

The net compromising probability will be:

\[
p_{\text{comp}} = p_{\text{comp.Re}} \cdot p_{\text{comp.Re}}
\]

\[
p_{\text{comp}} = (p_{\text{occu.Re}} + p_{\text{sick.Re}}) \left( 1 - t_1 \cdot \frac{1-p}{n-p-t_2} \right) \frac{n_p^r}{t_2} \left( \frac{n_p^r}{t_2-i} \right) + \frac{k}{n_p \text{health} + k}
\]

\((19)\)

The above analytical study is for the first round of self-healing after ADV leaving, the sick sensors near the boarders of cluster try to self-heal using SH scheme. However, from the second round and after applying the mobility scheme within the cluster, so, our analytical study will transfer from network level to cluster level. After mobility and fusion of healed and sick sensors, all sick sensors will have health neighbours. Therefore, the self-healing will start again but it will be within the cluster. Also for simplicity, we can consider only one type of peers, \(P_{\text{peers}}\) will be considered as the sponsors, they will initialize and offer their help for a sick sensors, for a cluster of \(k\) sick sensors and \(n_{hc}\) healed sensors, the probability to select \(t\) of \(P_{\text{peers}}\) will be:

\[
P_{\text{peers}} = \frac{t}{n_{hc}}
\]

\((20)\)

The sick \(s_i\) will fail to self-heal for two events \((A_p, B_p)\). Event \(A_p\); the probability that there is no any \(P_{\text{peers}}\):

\[
P(A_p) = 1 - P_{\text{peers}} = 1 - \frac{t}{n_{hc}}
\]

\((21)\)

Event \(B_p\); the probability that the ADV intercepts the contribution of \(P_{\text{peers}}\):

\[
P(B_p) = P_{\text{peers}} \cdot p = \frac{t}{n_{hc}} \cdot p
\]

\((22)\)

The probability that \(s_i\) is still sick at round \(r + 1\) is:
\[ p_{\text{sick,pro}}^{r,r+1} = (P(A_p) + P(B_p))^{n_{hc}} \]  
\[ n_{hc}^r = \begin{cases} k, p^{r-1}_{health} & r > 1 \\ 0 & r = 1 \end{cases} \]

\[ p_{\text{sick,pro}}^{r,r+1} = \left(1 - \frac{t}{n_{hc}} + \frac{t}{n_{hc}} \cdot P\right)^{k p^{r-1}_{health}} = \left(1 - t \cdot \frac{1-p}{n_{hc}} \right)^{k p^{r-1}_{health}} \]

\[ p_{\text{sick,pro}}^{r} = (p_{\text{occu,pro}}^{r-1} + p_{\text{sick,pro}}^{r-1}) \cdot p_{\text{sick,pro}}^{r+1} \]

\[ p_{\text{occu,pro}}^{r} = \frac{k}{n_{p_{health}} + k} \cdot \frac{A_c}{A_n} \]

Where \( A_c \) and \( A_n \) are the cluster and network areas respectively. The probability of \( s \) is compromised for the next rounds will be:

\[ p_{\text{comp,pro}}^{r} = p_{\text{sick,pro}}^{r} + p_{\text{occu,pro}}^{r} \]

\[ p_{\text{comp,pro}}^{r} = (p_{\text{occu,pro}}^{r-1} + p_{\text{sick,pro}}^{r-1}) \cdot \left(1 - t \cdot \frac{1-p}{n_{hc}} \right)^{k p^{r-1}_{health}} + \frac{k}{n_{p_{health}} + k} \cdot \frac{k}{n} \]

where the ratio \( A_c / A_n \) is equal to \( k / n \).

**IV. THEORETICAL AND NUMERICAL RESULTS DISCUSSION**

In this section, the theoretical expressions are used to test the performance of the SH-CCM scheme and compare its performance with the schemes proposed in [9]. The theoretical results of the analytical model are obtained using \( N = 500, p = 0.2, k = 100 \). Fig. 1 shows the probability of \( B_{se} \) to be compromised against the number of rounds for the proposed analytical analysis of SH-CCM scheme and the simulation analysis of SH-CCM in [9]. It is clear that the analytical analysis results converge the simulation analysis results in [9] especially when the network reaches steady state, these results validate the analytical analysis.

Figure 2 shows the probability of \( B_{se} \) to be compromised against the number of rounds for SH-CCM analytical model and CHSHRD [1]. This figure ensures that the proposed scheme achieves two performance enhancements. First, the proposed scheme wins the game against the ADV early, where the network reach steady state from round two comparing to round five in the case of CHSHRD scheme. Second, the proposed SH-CCM scheme reduces the probability of \( B_{se} \) to be compromised by about 38.5% when compared with the CHSHRD scheme.

Figure 3 shows the probability of \( B_{se} \) to be compromised against adversary capability. This figure ensures that the proposed scheme achieves better security when compared with the CHSHRD scheme especially at higher adversary capability. Figures 4 and 5 show the probability of \( B_{se} \) to be compromised against the number of rounds and adversary capability, respectively for different values of sponsors (t). It is clear that as the number of sponsors’ increase, the results curves approaches each other which emphasis the fact that, a certain number of sponsors is sufficient to perform self-healing and the self-healing algorithm can stand well against the ADV. This number is six sponsors (t = 6) in [8, 27]. On the other hand, the obtained results show that for (t ≥ 4) the performance approximately the same, this ensure that our proposed scheme has a better performance with respect to the overhead communication.

Figure 6 shows the probability of \( B_{se} \) to be compromised against number of rounds for different values of adversary capability. It is clear that the proposed model can stand well even at higher value of adversary capability. Also from the above figures it is clear that the performance of the proposed scheme against the number of rounds will saturated as the number of rounds increase. Saturation means that the proposed scheme stands well against the adversary (i.e., wins the game against the attacker), so we can say that the proposed scheme provides sustainable self-healing.
V. Conclusion

In this work, an analytical analysis of SH-CCM scheme for sensor regaining secrecy and high data reliability in UWSNs was estimated. The proposed scheme combines both cooperation and infusion of mobility with cooperative hybrid self-healing schemes to enhance the ability of security regaining and maximize both security level of data and guarantee probabilistic $BSe$ and compromised probability. In addition to the above improvements, the proposed scheme will save rounds of cooperation and self-healing process required for self-healing, hence it also enhances the efficiency of the entire network. Analytical results ensure the efficiency of the proposed scheme. The proposed scheme also reduces the overhead communication by using the minimum number of sponsors. Comparing with other schemes, the proposed scheme was more forceful and outperforms the others schemes [1, 27].

![Fig. 1: The probability of $BSe$ to be compromised against the number of rounds.](image1)

![Fig. 2: The probability of $BSe$ to be compromised against the number of rounds.](image2)

![Fig. 3: The probability of $BSe$ to be compromised against the Adversary capability.](image3)

![Fig. 4: The probability of $BSe$ to be compromised against the number of rounds.](image4)
REFERENCES


