CHAPTER 5

MSRD-FL: FUZZY LOGIC BASED MOBILE SINK REPLICA DETECTION SCHEME FOR WIRELESS SENSOR NETWORKS

5.1 INTRODUCTION

WSNs offer the best solution for monitoring areas that are not accessible and for which it is harder to deploy the traditional wired network. Environmental monitoring and vehicle monitoring applications use WSNs for real time data (Yun & Won 2012). WSNs are easy to deploy (Philip Chen et al 2012). The small size of the sensor nodes makes WSNs versatile for deployment in most applications. Data aggregation is a critical task in WSNs. In static WSNs, multi-hop transmission of the sensed data is unavoidable.

In multi-hop transmission, sensor nodes use critical resources in data forwarding, rather than their primary function of sensing the parameter assigned. Mobile sink deployment in WSNs has made data collection and node revocation more powerful. Because of their functioning characteristics, sensor nodes are physically unmonitored, and consequently vulnerable to a variety of attacks. It is crucial to ensure the security as well as resilience of WSNs because they are ideally suited for various applications. A large number of key management schemes are discussed in the literature (Gu et al 2011) for securing WSNs.
Node capture and node replication attacks are considered serious threats in WSNs. Various node capture and replica detection schemes are discussed in the literature. Many existing schemes have only considered static WSNs. Very few researchers have addressed the security aspects of mobile WSNs. The role of mobile sinks is vital in data aggregation and network maintenance of modern WSNs with mobile nodes and mobile sinks. Many WSNs deploy only one mobile sink for data aggregation. Compromise of mobile sinks by powerful attacker leads to compromise of entire WSNs.

Mobile sinks travels in WSNs in specified trajectories to gather the sensed information from legitimate nodes. The adversary captures the sensor nodes due to their limitations in physical security like being prone to tampering. Successful node capture reveals the node ID, cryptographic information like keys and neighbor node information to the adversary. The adversary takes advantage of the node capture information to launch a variety of attacks, of which node replication is a powerful attack. The adversary redeploy the captured node into the network, which misbehaves and disrupts the network's operations.

The replicated mobile sink mimics an authentic mobile sink and communicates with the legitimate components of the network. Some researchers have addressed the mobile sink replication attack in WSNs by proposing key management based security mechanisms. Key management involves generation, distribution and revocation of the keys.

This research examines the replication or clone attack with respect to mobile sinks in WSNs. To address this problem, a security mechanism called mobile sink replica detection scheme (MSRD–FL) based on fuzzy logic is proposed. The novel MSRD – FL exploits the mobile sink trajectories and their direct communicating components of the network with its parameters to establish secure connection. The proposed mechanism increases the efficiency
In WSNs for detecting the mobile sink replication attack, where the legitimate nodes are protected from establishing pair-wised key with the replicas of the mobile sinks. The MSRD-FL has been validated through simulation, security and threat analysis. Simulation results show that MSRD-FL detects the mobile sink replicas in WSNs more effectively than existing security mechanisms.

Figure 5.1 WSN with mobile sink replica

5.2 ASSUMPTIONS

This section describes the assumptions made in the proposed MSRD-FL.
5.2.1 Network Assumptions

- All the sensor nodes are static
- Sensor nodes are not tamper proof
- Mobile sink travels in specified trajectories
- Bi-directional communication link
- No centralized monitoring
- Same session interval used for data collection between access point and mobile sink
- Nodes do not have knowledge of their locations

5.2.2 Adversary Assumptions

- Ability to eavesdrop on network communication
- Ability to compromise nodes
- Introduce replica of the mobile sink with known cryptographic information
- Capable of introducing multiple replicas of same mobile sink
- Can only introduce replicas of mobile sinks with same ID as legitimate sinks
Consider a large scale wireless sensor network comprised of one base station, some mobile sinks, limited access points and a large number of sensor nodes. The actual sensor node will sense the particular area of interest and forward that information towards the access point. Access points act as secondary data aggregation units that forward data to the mobile sink. Separate key pools are used to establish secure connections between sensor node, access point and mobile sink. Senior node access point uses the static polynomial key pool for secure connection establishment. Access point and mobile sink use mobile polynomial key pool for establishing connection. The basic connection establishment and key management of the proposed scheme were based on (Rasheed et al 2012). The adversary captures legitimate access points, then makes use of its cryptographic information to deploy replicated mobile sink in WSNs.

5.3 MSRD-FL: FUZZY LOGIC BASED MOBILE SINK REPLICA DETECTION SCHEME

The MSRD-FL proposes a fuzzy logic based mobile sink replica detection scheme for large scale WSNs. Access point parameters such as next hop communication, session interval for data transfer to mobile sink, mobile sink trajectory ticket, and freshness of the trajectory ticket are considered by the MSRD-FL. The access point parameters are used to detect mobile sink replication attack by the fuzzy logic technique.

MSRD-FL identifies indirect communicating access points with the mobile sink, and isolates them with Mobile Polynomial Pool (MPP). The isolation of the access points is based on Figure 5.2.
Input: Routing table of the access point APi

if next hop of access point APi is MS Do nothing

else

    Indirect Communication Region (ICR) ← Log APi ID

Find APj which is next hop to the MS

Establish pair-wise key with APj using SPP instead of MPP

Hash ← MPP information in AP (which is in ICR)

End if

Figure 5.2 Isolating Indirect communication Region access points with MPP

Isolation of the indirect communication access points act as first level of MSRD-FL. Mobile polynomial pool is available only with access points which are in Direct Communication Range (DCR). For a successful mobile sink replication attack, adversary needs to identify access points which are in DCR with the mobile sink.

The critical data aggregation process involves the movement of the mobile sink in available trajectories. Mobile sinks follow trajectories to collect the access point data by establishing secure connections as shown in Figure 5.3. The mobile sinks have specific trajectories to reach maximum number of access points. The access points which are in DCR with a mobile sink in a one trajectory are in Indirect Communication Range (ICR) in another trajectory.
A matrix contains mobile sink trajectories and their corresponding access points' information resides with the mobile sink. Mobile sink use the trajectory matrix in data aggregation. The matrix is generated as per Figure 5.4 and is shown in equation (5.1).
Input: Number of trajectories (T) and Number of Access points (NAP)

Generate a matrix of size $G_{ij} = T \times NAP$

for all $T_j$

if $A_{Pi}$ is in DCR of MS then

$G_{ij} = 1$;

Else

$G_{ij} = 0$;

End if

End for all

Figure 5.4 MS matrix with APs region

Let $G = \begin{pmatrix} G_{11} & \cdots & G_{15} & \cdots & G_{1T} \\ \vdots & \ddots & \vdots & & \vdots \\ G_{x1} & \cdots & G_{xT} \end{pmatrix}$ \hspace{1cm} (5.1)

The mobile sinks identify the number of available trajectories and generate a ticket of specific length, which is issued to every access point. The ticket reveals the mobile sinks' movement in the successive iteration for data collection and future trajectories. Assuming a mobile sink with three trajectories and generated ticket length of three all possible combinations of trajectories are shown in Figure 5.5.
Total number of possible combinations of trajectory sequence of a mobile sink is $T^T$.

Trajectory ticket sample = (1 2 3)

Ticket sample reveals that for the next three iterations, mobile sink will traverse the network in the order T1, T2 and T3.

Access points forward the aggregated data to the mobile sink at regular sessions. The session intervals in a trajectory for data transfer to mobile sink will be the identical. Access points data forwarding intervals $t_1$, $t_2$, $t_3$, ..., $t_n$ corresponds to trajectories T1, T2, T3,...,TN. The average time taken for one time communication with the mobile sink is $t_{\text{threshold}}$. 

Figure 5.5  Possible trajectory combinations
**Procedure** Replicated_mobile_sink_claim

claim ← (ID_r, curr_ticket_seq, session_time())
RMS claim → access_points in DCR

**end procedure**

**procedure** Received_claim_at_AP

if claim then

if bad ID then

discard claim

else

do check

SM_ticket_check (claim (_, curr_ticket_seq, _))

end do

if claim (_, curr_ticket_seq, _) → invalid ticket

discard claim

trigger alarm procedure for ID_r

else

do check

avg_session_time (claim(_, _, session_time()))

end do

if claim (_, _, session_time()) → exceed t_threshold

discard claim

trigger alarm procedure

---

**Figure 5.6** MSRD-FL algorithm
else
trigger key_setup procedure for ID,
end if
end if
end if
end if

Procedure alarm
If invalid ticket or ID or session_time() then
Broadcast_replica (ID, curr_ticket_seq, session_time()) → neighbors
Store detected_replica( ID, curr_ticket_seq, session_time())
Request_new_ticket
end if
end procedure

Procedure received Broadcast_replica
Store detected_replica( ID, curr_ticket_seq, session_time()) in memory
end procedure

Procedure received detected_replica
Discard claim
Trigger alarm
end procedure

Figure 5.6 (Continued)
The pseudo code of the proposed mobile sink replica detection is described as Replica Detection Scheme (RDS) in Figure 5.6.

A fuzzy logic system is implemented for detecting mobile sink replication attack. Access points determine the replica connection probability to start a secure session with mobile sink that depends on the polynomial-pool, DCR-check, requested session interval and ticket freshness as shown in Figure 5.7.

Figures 5.8 to 5.13 display the membership functions of the crisp input of the fuzzy model and the crisp output function connection probability. Membership functions possess value between 0 to 1 in accordance with Figure 5.6. A popular fuzzy inference method called Mamdani method was employed, consisting of if-then rules to produce fuzzy output as shown in diagram Figure 5.14. Centroid defuzzification method is used to convert the fuzzy outputs to crisp outputs.

The membership function of the polynomial pool is defined by the linguistic values static pool and the mobile pool as shown in Figure 5.8. Based on the request, the legitimate node validates the key IDs and correlates with other security parameters considered for replica detection.

Access point direct communication with the mobile sink is an important parameter to be considered in the proposed MSRD-FL. The membership function of the DCR check is defined by the linguistic values far medium and near as shown in Figure 5.9.

The membership function for the ticket freshness is represented by the linguistic values available and not available as shown in Figure 5.10.
Figure 5.7  Fuzzy logic system

System: MSRDFL; 5 inputs; 1 output; 14 rules

Figure 5.8  Fuzzy membership function for polynomial pool
Figure 5.9  Fuzzy membership functions for DCR-check

Figure 5.10  Fuzzy membership functions for ticket freshness
Figure 5.11  Fuzzy membership functions for session interval

Figure 5.12  Fuzzy membership function of ticket check
The membership function for the input variable session interval is as shown in the Figure 5.11 and defined by the linguistic values unacceptable, acceptable, and exact. The input variable ticket check is defined by the membership functions as shown in the Figure 5.12. The membership function for the replica connectivity is as shown in the Figure 5.13 and represented by linguistic values low, medium and high.

Table 5.1 Sample rule base

<table>
<thead>
<tr>
<th>DCR-check</th>
<th>Session-interval</th>
<th>Polynomial pool</th>
<th>Ticket check</th>
<th>Freshness</th>
<th>Replica connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near</td>
<td>Exact</td>
<td>Mobile pool</td>
<td>pass</td>
<td>Available</td>
<td>High</td>
</tr>
<tr>
<td>Far</td>
<td>Exact</td>
<td>Mobile pool</td>
<td>pass</td>
<td>Available</td>
<td>Low</td>
</tr>
<tr>
<td>Near</td>
<td>Exact</td>
<td>Mobile pool</td>
<td>pass</td>
<td>Unavailable</td>
<td>Low</td>
</tr>
<tr>
<td>Near</td>
<td>Exact</td>
<td>Static pool</td>
<td>pass</td>
<td>Unavailable</td>
<td>Low</td>
</tr>
<tr>
<td>Near</td>
<td>Exact</td>
<td>Mobile pool</td>
<td>Fail</td>
<td>Unavailable</td>
<td>Low</td>
</tr>
</tbody>
</table>
Figure 5.14   Rule viewer for the proposed MSRD-FL scheme
Figure 5.15  Rule viewer for the proposed MSRD-FL scheme
A rule base is as shown in Table 6.1. Based on these rules the fuzzy interface generates the crisp output of the system. This crisp output is the replica connection probability of the proposed MSRD-FL scheme. The fuzzy rules are optimised as per the requirement of the MSRD-FL and a total of 14 rules are created to govern the replica connection with the legitimate access points in the network.

The crisp fuzzy output drives the access point to identify the replica of the mobile sink. Figure 5.15 shows a mobile sink send request message m1 to legitimate access point for connection establishment. The legitimate access point processes m1 in accordance with the MSRD-FL, the crisp output of fuzzy model validates the request m1. Thus, a valid m1 request makes access point to respond back with message m2 and establish secure connection with mobile sink. Invalid request m1 makes access point send the alarm message to the network as shown in Figure 5.17.

![Figure 5.16 Communication between mobile sink and access point](image)

**Figure 5.16 Communication between mobile sink and access point**
The memory usage for fuzzy logic interface is as follows

- The membership values \( (M_v) \) of each fuzzy set \( (F_s) \) have to be stored in the memory. The membership value is of length 4 bytes. The total memory required to store fuzzy set is \( 4 \times M_v \times F_s \).

- The membership functions are stored in the memory as index numbers of size 2 bytes.

- Memory required for rule base = \( 2 \times \text{number of rules} \times (I_n + I_c) \) where \( I_n \) is the number of inputs to the fuzzy interface and \( I_c \) is the number of outputs of the fuzzy interface. The memory usage to store rule base is 0.16 KB.

- Fuzzy logic interface system is more suitable for memory constrained networks as discussed in the literature.

**Figure 5.17  Communication between replica of mobile sink and access point**

The memory usage for fuzzy logic interface is as follows
5.4 CONCLUSION

Mobile sink replication attacks can compromise the entire network in a very short time. The longer the replicated sink is present in the network, the greater the damage to the network. Tolerating mobile sink replication attack is challenging, hence a security scheme called MSRD-FL has been proposed. The simulation results prove that the proposed scheme increases the resilience of the sensor network against mobile sink replication attack.