CHAPTER 5

TIMESTAMPED FIREWALL FOR HOMOGENEOUS WIRELESS SENSOR NETWORK

This chapter presents a Timestamp Firewall based misused key detection (TFMKD) protocol for hierarchical routings. In TFMKD information to the BS goes through Firewall which detects misused key by itself and if it finds any misused key then prepare a committing message and send it to the BS for final detection. In TFMKD, a Firewall SN is selected on timestamp basis which plays the role of a CH and misused key detector. We have also compared TFMKD with some existing schemes.

Rest of the chapter is organized as follows. Section 5.1 presents issues related to mis-used key detection and revocation from the network. In Section 5.2 system model is given and Misused Key Detection Protocol is described in Section 5.3. Simulation model is given in Section 5.4 followed by result and discussion in Section 5.5. Finally summary of the work done is given in Section 5.6.

5.1 Issues

Many efficient key management mechanisms are available in literature [27, 28, 103] and if these keys are compromised, some mechanisms are also available in literature [112, 113] to detect and revoke these keys from the network. In these schemes, for each received data from a SN, CH transmits an additional message to the special SNs for detecting misused key. If these schemes are applied to the hierarchy routings, overhead of detecting misused key is concentrated on the CH. So, dead time of the CH becomes very short, finally, life time of the network is reduced.
5.2 System Model

In TFMKD, Firewall is a SN which receives all the sensed data from other SNs within the cluster like CH, aggregate these data and forward the aggregated data to the BS. One of the SNs within the cluster is selected on timestamp basis to work as a Firewall. All the sensed data within the cluster goes to BS through the Firewall. On receiving data from SNs within the cluster, Firewall authenticate data packet, perform key verification and if everything is alright, it sends the aggregated data to the BS otherwise it prepare a report message and send it to the BS for final key verification. The process is shown in Figure 5.1.

![Figure 5.1 Information exchange between Firewall and BS.](image)

We have assumed that all SNs are distributed in randomized manner in a square region and the network has the following properties:

- There exists a unique BS, located far away from the network.
- Each SN has a unique identity.
- SNs can not move after being deployed.
- Network is homogeneous i.e. all SNs having the same computing and communication capacity.
- BS is non compromised SN.

5.3 Misused Key Detection Protocol

In TFMKD all information goes to the BS through Firewall which detects misused key partially. TFMKD consists of two phases for identifying the misused key. The phase-I is performed at the Firewall for partial detection of misused key. The phase-II is operated at the BS for preventing the Firewall from misdetection of the misused key. The following conventions are used in the TFMKD.
\{u, v\}: Identity of SN u and v respectively

\( C_{u,v} \): Cumulative hash value

\( K_u \): Individual key of SN u, shared with BS

\( K_{u,v} \): Pair-wise key shared between SN u and SN v

\{V_1, V_2\}: Committing values computed by using Equation (5.2)

\{MAC_1, MAC_2\}: Message Authentication Code

### 5.3.1 First Phase of Protocol

To perform the first phase, TFMKD uses the cumulative hashed value \( C_{u,v} \) which provides a history of the messages exchange between the node u and Firewall node v. TFMKD also uses a Firewall for partial detection of the misused key. The Firewall reduces the overall message exchanged within the network in the detection of misused key. The \( C_{u,v} \)'s are separately maintained at each sides, i.e., at node u and Firewall node v. The initial value of \( C_{u,v} \) is 0.

The value of \( C_{u,v} \) are updated by using Equation (5.1) when u sends message M to v or the node v receives message M from u. After updating the value of \( C_{u,v} \), node u sends \{M \parallel MAC_1\} to the Firewall node v with probability 1-p, where \( MAC_1 \) is MAC of M using pairwise key \( K_{u,v} \), on receiving the message from u Firewall node v also update its \( C_{u,v} \). If the messages between the node u and Firewall node v are not modified or not inserted, or not misused by an attacker, the two \( C_{u,v} \)'s are same at each side. The sender u then computes \( V_1 \) and \( V_2 \) by using Equation (5.2), where \( K_{\text{unique}} \) is the pair-wise key \( K_{u,v} \) and \( K_u \) respectively and sends \{u\parallel(M, V_1, V_2) \parallel MAC_2\} MAC_3 to the Firewall node v with probability p and updates its \( C_{u,v} \) as earlier.

\[
C_{u,v} = H(M \parallel C_{u,v}) \quad \text{... (5.1)}
\]

\[
V = H(C_{u,v} \parallel K_{\text{unique}}) \quad \text{... (5.2)}
\]

The MAC_3 is MAC of \{u\parallel(M, V_1, V_2) \parallel MAC_2\} generated by using pair-wise key \( K_{u,v} \) and MAC2 is MAC of \( (M, V_1, V_2) \) generated by using \( K_u \). On receiving, Firewall node v also update its \( C_{u,v} \) and authenticate message (2); if authentication succeed, it computes \( V_1' \) as \( V_1' = H(C_{u,v} \parallel K_{u,v}) \), where \( C_{u,v} \) is its own \( C_{u,v} \). Figure 5.2 presents misuse key detection mechanism. If \( V_1 = V_1' \), Firewall node v stop the process, however if the message M is modified by an adversary, the value of \( C_{u,v} \) at sender u and at Firewall node v will be different and so the value of \( V_1 \) and \( V_1' \) will be different. In this case Firewall...
node v prepare message (3) as shown in Figure 5.3 and send it to the BS for final detection and phase-II of the protocol is initiated. Like other SNs Firewall node v may also be compromised by an attacker. If the Firewall node v is compromised and cheats, it can cheat the detecting scheme. To overcome this, TFMKD selects Firewall on timestamp basis so that if the Firewall node v is compromised, in the next timestamp it has been changed and now u delivers the message to this newly selected Firewall and misused key will be detected.

![Diagram](image)

**Figure 5.2** Working of first phase of Protocol.

### 5.3.2 Second Phase of Protocol

The second phase of TFMKD is used to confirm result of detection and to replace misused key with new key. To perform the phase-II of TFMKD, the Firewall node v inform to the BS about detection of misused key. In TFMKD, the Firewall node v transmits the reporting messages to the BS. The Firewall node v can transmit reporting message with delivering data. So, the Firewall node v working as CH can reduce the overhead of reporting message. Figure 5.3 explores phase-II of the protocol. The Firewall node v, prepares a reports message when it detects a misused key and send it to the BS as shown in Figure 5.3.

![Diagram](image)

**Figure 5.3** Working of second Phase of Protocol.

$C_{u,v}$ is the cumulative hashed value maintained at the Firewall node v and Committing value $V_2$ of report message is generated by the sending node u.
The MAC\textsubscript{4} of message is MAC of \{u||v|| C\textsubscript{u,v} ||V\textsubscript{2}\} by using individual key K\textsubscript{v}. The BS checks MAC\textsubscript{4} when it receives reporting messages. If the verification of the MAC\textsubscript{4} succeed, the BS calculates V\textsubscript{2}' = H(C\textsubscript{u,v} || K\textsubscript{u}). If V\textsubscript{2} and V\textsubscript{2}' are not same each other, the BS decides that the key is being misused and notifies this facts to SN u and v, generates new pairwise key between u and v and transmits it in the WSN. The TFMKD is not concerned with the mechanism of scheduling of Firewall node v and new pair-wise key generation and notification.

5.4 Simulation Model

We will compare the energy efficiency of TFMKD with that of the Liu and Dong scheme \cite{112} and Park, Kim, Han and Chung scheme \cite{113}. To verify how presented scheme is more efficient than the Liu and Dong’s scheme and Park, Kim, Han and Chung scheme, we have simulated the cumulative energy dissipation of the CH and the other SNs within that cluster.

For realistic, our simulation uses the first order radio model \cite{9, 10} as the communication model. Equation (5.3) and (5.4) represent the energy dissipation when a SN sends or receives an l-bit message.

\begin{equation}
E_{\text{trans}} = \begin{cases} 
 l \times (E_{\text{elec}} + E_{fs} \times d^2), \text{if } d \leq \sqrt{\frac{E_{fa}}{E_{mp}}} \\
 l \times (E_{\text{elec}} + E_{mp} \times d^4), \text{if } d > \sqrt{\frac{E_{fs}}{E_{mp}}} \quad \ldots \quad (5.3)
\end{cases}
\end{equation}

\begin{equation}
E_{\text{recieve}} = l \times E_{\text{elec}} \quad \ldots \quad (5.4)
\end{equation}

The following are the simulation parameters considered for the implementation of the developed scheme.

- The distance between the BS and the network is taken as 125m.
- Size of message is 80 bytes.
- Free space attenuation coefficient (E\textsubscript{fs}) is 10 pJ/bit/m\textsuperscript{2}.
- Multi path attenuation coefficient (E\textsubscript{mp}) is 0.0013 pJ/bit/m\textsuperscript{4}.
- Electronic power (E\textsubscript{elec}) is 50 nJ/bit.
• Size of committing value 8 bytes.
• Size of $C_{uv}$ is 8 bytes.
• Size of node ID 4 bytes.
• Size of MAC 8 bytes.
• Number of SNs within cluster is 11.
• Average distance between SNs within cluster and Firewall node (i.e., CH) is assumed to be 7.5m.
• Cluster area 10m$^2$.

5.5 Result and Discussion
This Section present a comparative study of TFMKD in respect of cumulative energy consumption with the earlier work proposed by Liu and Dong and Park, Kim, Han and Chung scheme. Figure 5.4 shows cumulative energy consumption in the message transmitting SNs; it presents that developed scheme is more efficient than Liu and Dong scheme and similar to Park, Kim, Han and Chung scheme. TFMKD reduces energy consumption approximately 11% as compared to Liu and Dong scheme.

Figure 5.5 shows cumulative energy consumption in the receiving node, i.e., Firewall node. From the result in Figure 5.5 we can see that presented scheme is efficient as compared to Liu and Dong scheme and equal to that of the Park, Kim, Han and Chung scheme. Developed protocol reduces energy consumption around 19% as compared to Liu and Dong scheme.

Figure 5.6 shows cumulative total energy consumption; it represents that the developed protocol is efficient than both earlier proposed protocol. Presented scheme reduces around 18% energy consumption as compared to Liu & Dong scheme and around 9% as compared to Kim, Han and Chung scheme.

In the both earlier schemes around 30% SNs, works as a special node in the detection process, which are not required in TFMKD protocol. In TFMKD protocol these extra SNs may be used either to cover more deployment area or may be deployed in another interval (i.e., in case of group deployment) to extend the network life.
Figure 5.4 Cumulative energy consumptions in SNs.

Figure 5.5 Cumulative energy consumption in cluster-head.
Figure 5.6 Cumulative total energy consumptions.

5.6 Summary

This chapter presents a protocol to detect misused keys within the network, revoke them from network and assigned a fresh keys to the compromised SNs. In the protocol, firewall which is one of the SN within the cluster, is selected on time stamp basis, to detect misused keys if any and sends a report message about this undesirable activity to the BS and plays the roll of CH as well. Energy consumption in presented protocol is less than earlier works discussed in the literature and also significantly decreases overhead within the cluster. In the next chapter a secure and energy efficient adaptive routing protocol is presented.