CHAPTER 6

ANONYMOUS SECURE COMMUNICATION
SCHEME

6.1 INTRODUCTION

Wireless sensor networks (WSNs) are used in various fields for performing different applications. In every applications sensor nodes collects sensitive data from surrounding environment as the data are the basis for enabling applications and services in WSNs. The sensor nodes are constrained with low battery power. During operation sensor nodes are deployed in larger number in a hostile environment with an expectation to survive for a long period. The unstable wireless link and the limited energy of the sensor nodes cause frequent changes in the communication path due to link failure or node failure. In addition, the communications done in WSNs may be subjected to traffic analysis and other Denial of Service (DoS) attacks through compromised en-route nodes along the path.

To protect the event information during transmission it is essential to route data through an optimal path and hide traffic details from being exposed to the unauthorized node during data transmission. To select an optimal path it is necessary to consider various constraints other than focusing on a single constraint in path construction and attacks through traffic analysis which can be prevented by means of anonymous data transmission. It is necessary to provide security along with anonymity for the data in transit.
Different security approaches are required at different instants based on the environment where it is to be applied and based on the resources available for providing the security measures. While designing security mechanism, it is necessary to consider the limited resources available in sensor nodes to achieve maximum security through the limited resources available (Yang et al 2006). The protocols to be designed should focus on the drawbacks and limitations of existing security protocols that affects the performance of the sensor network. Further the protocols to be proposed should address the issues that occur during cryptographic operations such as key generation, key sharing and secure data sharing (Hua-Yi Lin 2009).

Anonymity can be achieved in the proposed scheme through dummy traffic representation instead of specifying the real source and destination information in the packet to be transmitted. Moreover, in the proposed scheme to address the key sharing issues cryptographic keys are pre-distributed to the corresponding sensor nodes before initiating communication. This scheme avoids the necessity to have a secure channel to share the authentication information additionally to en-route nodes along with the selected path. Moreover, this scheme achieves link level authentication and end-to-end security without auxiliary message exchange between the sensor node and BS.

Further, the proposed scheme uses the principle of fuzzy logic to select an optimal path to be used for secure data transmission. Hence, the proposed Anonymous Secure Data Transmission Scheme (ASDTS) which is efficient in establishing secure communication in WSNs with minimum computation and communication overhead.
6.2 NEED FOR PROVIDING ANONYMITY ALONG WITH SECURITY SERVICES

As the demand for applications of WSNs get increased the vulnerabilities caused by the adversaries to sensor nodes also gets increased. The unattended nature of sensor nodes during operation makes them susceptible to different types of passive and active attacks such as eavesdropping, false data injection, false endorsement, data misdirection etc (Wang et al 2009). Security services such as confidentiality, authentication and integrity are required to protect the sensor nodes from these attacks. But in some situation an adversary may collect the traffic details continuously for a particular period and perform traffic analysis attack using the collected information to know about the source and destination nodes involved in the communication (Xie et al 2011).

Security services such as confidentiality and authentication are not sufficient to protect the contextual information stored in the header portion of a packet on transit (Cao et al 2009). But these security services are used only for protecting the data part of the packet. Also the information maintained in the header portion cannot be encrypted due to multi-hop routing technique followed in WSNs.

But it is essential to protect the privacy of source and destination nodes involved in a communication which protects them from the vulnerabilities caused during data transmission (Mehta et al 2011; Park et al 2011). Anonymity is a security service used to prevent such types of attack (Ei Defrawy & Tsudik 2011). Anonymity prevents the adversary from knowing about the source and destination identity by hiding the identities maintained in the packet header (Misra & Xue 2006a, 2006b). The proposed scheme is able to achieve the security service such as anonymity, confidentiality and authenticity in establishing secure communication (Misra
et al 2009). Hop-by-hop anonymous secure communication is achieved through the proposed scheme. This scheme is highly resilient to attack which is caused by monitoring the relationship between successive packets transmitted along with a fixed path (Shen & Zhao 2013).

6.2.1 Benefits of Link Level Authentication

Communications done through WSNs is open to everyone. Any sensor node in WSNs is allowed to participate in the communications performed within the network. Authorized and unauthorized users may be present within the network. Unauthorized users may perform malicious activities over the data in transit and prevent the data from safely reaching the Base Station (BS). It is essential to authenticate the data as well as origin as the data received by the BS may be used for some critical situations.

In some applications data collected by sensor nodes may be used by an outside user. Hence it is necessary to provide effective authentication mechanism to perform secure communication (Fan et al 2010; Wang & Liu 2011; Tameem & Shukor 2012). Authentication mechanism ensures the authenticity of nodes involved in communication and validates the authentication information exchanged between the sensor nodes (Chun-Tai et al 2009; Hyun-Sung & Lee 2009). Mechanism for authentication may be password based authentication, message authentication code (MAC) and identity based authentication. Maintaining and storing password based authentication is a challenging issue.

MAC based authentication uses cryptographic functions to generate MAC code and is a short piece of information used to authenticate a message (Rosales & Garcia 2009). Due to the multi-hop communication and in-network processing behaviour owned by WSNs it is necessary to perform security operations at every hop (Ozdemir & Cam 2010). Hop-by-hop
authentication of the report in transit is required to detect and drop fabricated event report without being forwarded to the BS.

6.2.2 Need for Fuzzy Model in Path Finding

Sensor nodes are battery powered with small memory and low processing power. Once deployed in an application specific region, sensor nodes are left unattended and are expected to function for a long period. To continue with the operation of sensor nodes for a long period it is necessary to save the limited battery energy from unnecessary damage caused by malicious nodes as the lifetime of a sensor node is based on its battery power.

Moreover, during communication it is essential to conserve energy of the forwarding nodes by reducing the extra energy consumption for establishing communication through the selected path. In the proposed scheme the constraints such as residual energy, traffic ratio and the count of neighbouring nodes should be considered on selecting forwarding nodes for establishing communication (Wang et al 2002). Due to the complex relationship existing between the constraints considered for routing, fuzzy based model is decided as the best approach for selecting optimized forwarding nodes along the path between the source and the BS (Babu et al 2012)

Most of the existing routing mechanisms are not efficient as they use a fixed routing metric for establishing an energy efficient path for data transmission (Moon & Cho 2012a). In WSNs due to the short transmission range owned by sensor nodes, they use multiple hops for forwarding their data to BS. This multi-hop communication increases the energy consumption rate of large number of nodes involved in data transmission. Fuzzy logic has
possible solution for dealing with such complex situation without the need for any complex mathematical approaches (Lee & Cho 2009). Also the rules and the logic followed in fuzzy based approaches are adoptable to dynamic environment (Sun et al 2008; Moon & Cho 2012a). Moreover, many design problems in communications systems are analysed perfectly using fuzzy logic due to its ability to handle imprecise nature of decision making environment.

Further, the problem with many of the existing routing protocols is the uneven dissemination of energy among the sensor nodes. The proposed ASDTS finds a routing mechanism in determining suitable forwarding nodes for constructing an optimal path. In this scheme a deterministic approach is followed to find efficient nodes for forwarding the data.

Further, forwarding nodes are selected based on three important criterions which decide about the lifetime of the sensor nodes. The factors considered for routing include residual energy, traffic ratio, number of neighbouring nodes and energy consumption for communication with neighbouring nodes. Fuzzy logic deals with analysis of information using fuzzy sets. Fuzzy sets are defined as the range of real values based on a domain.

6.3 PROPOSED SECURE COMMUNICATION SCHEME

In the proposed ASDTS framework, security can be enforced through an effective encryption and authentication mechanism along with ensuring privacy of the data on transit through anonymity. Moreover, proposed scheme ensure energy efficiency with maximum network lifetime. Also it increases the strength of security without the need for auxiliary message exchange between communicating entities.
Further, this scheme is efficient in establishing secure communication with respect to computation and communication cost by providing the security requirements when needed. The proposed scheme is executed in three different stages. The Phases of the proposed scheme are as follows.

i) Route discovery phase

ii) Secure session setup phase

iii) Anonymous and secure communication phase

In the first phase, a fuzzy logic based approach is used in selecting an energy efficient and optimized route for establishing secure communication. The main objective here is to minimize traffic, balance energy with the nodes involved in communication to prolong the network lifetime. In the second phase, the BS prepares and distributes secret key, witness key and other security relevant information to the selected forwarding nodes and the source node to achieve security during data transmission.

The purpose of the second phase is to achieve the security services confidentiality and authentication during communication. The third phase ensures anonymity and security in data transmission. This phase mainly focuses on increasing the privacy and secrecy of the data on transit.

6.3.1 Route Discovery Phase

In the proposed scheme routing is done by means of a fuzzy logic based approach. In this scheme fuzzy logic controller is used in selecting an optimal forwarding node. When a source node is triggered by an event, it needs to report event related information to the BS. Before forwarding the
event information source node needs to determine an optimal path for data transmission. Therefore source node broadcasts a route request message to one hop neighbour nodes. The one hop neighbour nodes receiving the request message respond with a reply message including its residual energy, count of neighbour nodes and the traffic ratio computed based on the previous communication done.

Each node determines its residual energy based on the energy consumed for transmitting and receiving packets. Energy consumed by a node for transmitting ‘b’ bit packet to the destination in a distance ‘d’ is given by Equation (6.1)

\[ E_{Tx} (b, d) = b * E_{elec} + b * d^2 * E_{amp} \]  

Likewise the energy consumed in receiving ‘b’ bit packet is given by Equation (6.2)

\[ E_{Rx} (b) = b * E_{elec} \]  

Where \( E_{elec} \) is the energy dissipated to transmit or receive by electronics and \( E_{amp} \) is the energy dissipated by power amplifier. Similarly each node determines its traffic ratio as given in Equation (6.3) as ratio of number of packets successfully received to the total number of packets send to the nodes with a time period. Also each node determines their neighbour information by periodically broadcasting ‘Hello’ packets.

\[ Traffic \ Ratio = \frac{\text{No. of packets received}}{\text{Total packets send}} \]  

(6.3)
Source node receives the reply message containing the required constraints and uses fuzzy logic based approach to select suitable forwarding node to forward the data. The architecture of a fuzzy logic controller is illustrated in Figure 6.1. The input values to be fed to the fuzzifier are 1) the residual energy of the node 2) traffic ratio of the node and 3) number of neighbouring nodes for the node.

![Figure 6.1 Architecture of fuzzy logic controller](image)

The input values (crisp) received by the fuzzifier are transformed into grades of membership for linguistic terms of fuzzy sets by means of a fuzzifier. The input factors and their fuzzy membership functions are represented through the Figure 6.2. Fuzzy sets are described by range of values called domain. Residual energy of a node represents the remaining energy level of a node. It has three fuzzy sets Low, Medium and High and its value exists between 0 and 2 Joule. Traffic ratio defines the ratio of number of packets successfully received to the total number of packets sent. Traffic ratio has three fuzzy sets Poor, Average and Excellent.

Its value exists between 0 and 100%. Neighbour information represents the count of one hop neighbour of a node. It has three fuzzy sets Few, Medium and Large and its values are between 1 and 16. The fuzzified input values are represented through triangular membership function.
Figure 6.2 Fuzzy membership functions of for input and output
<table>
<thead>
<tr>
<th>Rule No.</th>
<th>Residual Energy</th>
<th>Traffic Ratio</th>
<th>No. of Neighbours</th>
<th>Selection Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>low</td>
<td>poor</td>
<td>few</td>
<td>fair</td>
</tr>
<tr>
<td>2</td>
<td>low</td>
<td>poor</td>
<td>medium</td>
<td>poor</td>
</tr>
<tr>
<td>3</td>
<td>low</td>
<td>poor</td>
<td>large</td>
<td>poor</td>
</tr>
<tr>
<td>4</td>
<td>low</td>
<td>average</td>
<td>few</td>
<td>fair</td>
</tr>
<tr>
<td>5</td>
<td>low</td>
<td>average</td>
<td>medium</td>
<td>fair</td>
</tr>
<tr>
<td>6</td>
<td>low</td>
<td>average</td>
<td>large</td>
<td>poor</td>
</tr>
<tr>
<td>7</td>
<td>low</td>
<td>excellent</td>
<td>few</td>
<td>fair</td>
</tr>
<tr>
<td>8</td>
<td>low</td>
<td>excellent</td>
<td>medium</td>
<td>fair</td>
</tr>
<tr>
<td>9</td>
<td>low</td>
<td>excellent</td>
<td>large</td>
<td>poor</td>
</tr>
<tr>
<td>10</td>
<td>medium</td>
<td>poor</td>
<td>few</td>
<td>fair</td>
</tr>
<tr>
<td>11</td>
<td>medium</td>
<td>poor</td>
<td>medium</td>
<td>poor</td>
</tr>
<tr>
<td>12</td>
<td>medium</td>
<td>poor</td>
<td>large</td>
<td>poor</td>
</tr>
<tr>
<td>13</td>
<td>medium</td>
<td>average</td>
<td>few</td>
<td>good</td>
</tr>
<tr>
<td>14</td>
<td>medium</td>
<td>average</td>
<td>medium</td>
<td>good</td>
</tr>
<tr>
<td>15</td>
<td>medium</td>
<td>average</td>
<td>large</td>
<td>fair</td>
</tr>
<tr>
<td>16</td>
<td>medium</td>
<td>excellent</td>
<td>few</td>
<td>good</td>
</tr>
<tr>
<td>17</td>
<td>medium</td>
<td>excellent</td>
<td>medium</td>
<td>good</td>
</tr>
<tr>
<td>18</td>
<td>medium</td>
<td>excellent</td>
<td>large</td>
<td>fair</td>
</tr>
<tr>
<td>19</td>
<td>high</td>
<td>poor</td>
<td>few</td>
<td>fair</td>
</tr>
<tr>
<td>20</td>
<td>high</td>
<td>poor</td>
<td>medium</td>
<td>fair</td>
</tr>
<tr>
<td>21</td>
<td>high</td>
<td>poor</td>
<td>large</td>
<td>poor</td>
</tr>
<tr>
<td>22</td>
<td>high</td>
<td>average</td>
<td>few</td>
<td>good</td>
</tr>
<tr>
<td>23</td>
<td>high</td>
<td>average</td>
<td>medium</td>
<td>good</td>
</tr>
<tr>
<td>24</td>
<td>high</td>
<td>average</td>
<td>large</td>
<td>fair</td>
</tr>
<tr>
<td>25</td>
<td>high</td>
<td>excellent</td>
<td>few</td>
<td>good</td>
</tr>
<tr>
<td>26</td>
<td>high</td>
<td>excellent</td>
<td>medium</td>
<td>good</td>
</tr>
<tr>
<td>27</td>
<td>high</td>
<td>excellent</td>
<td>large</td>
<td>fair</td>
</tr>
</tbody>
</table>
The fuzzified input values and fuzzy rule base are fed to the fuzzy inference system. The fuzzified input values are processed based on the fuzzy rule base by the fuzzy inference system. The proposed fuzzy inference system is in Mamdani’s form and relates linguistic inputs to fuzzy output based on defined fuzzy rule base. The rule base consists of a set of IF-THEN rules which relates input fuzzy variable to output fuzzy variable using linguistic variable. In the proposed scheme there are three fuzzy sets for each input factors and the rule base therefore consists of 27 rules. The rule based generated for proposed scheme is represented in Table 6.1.

The output value of the inference system will be the chance for selecting a node as a forwarding node. The possible fuzzy based output values can be Poor, Fair and Good. The output of the fuzzy inference system is in the form of linguistic expression which is to be modified into crisp values by defuzzifier. The defuzzifier converts the fuzzy value into a crisp output value. The output value may be the chance for selecting a node as forwarding node. The crisp output value for the Selection Rate (SR) is computed by centroid defuzzification method. The output value SR is given by Equation (6.4).

\[
Selection Rate (SR) = \frac{\sum_{i}^{n} R_{i} \cdot C_{i}}{\sum_{i}^{n} R_{i}}
\]  

(6.4)

Where \( R_{i} \) is the output corresponding to rule \( i \), \( n \) is the number of rules triggered in the fuzzy inference engine and \( C_{i} \) is the centre of the output membership function. The best forwarding node is the node which owns the maximum fuzzy value as the output and its selection rate should be greater than 75\%. The same process is repeated by the selected forwarding node to select its one hop forwarding nodes. This process is repeated until a node finds its one hop neighbour as the BS.
6.3.2 Secure Session Setup Phase

The main goal of this phase is to assign all security related parameters and other system parameters to the sensor nodes involved in communication. Moreover, the onetime secret key used for establishing secure communication is also generated in this phase. Operation of this phase is done in two stages, System initialization and key generation.

System initialization: Once the forwarding nodes along the path are identified, to ensure the authenticity of the nodes involved in communication BS assigns witness key $K_w$ to the selected forwarding nodes along the path. Moreover, the lifetime of the sensor nodes is partitioned into number of sessions. Each session may be assigned with a fixed time interval. Further, each node is assigned with unique secret key that is shared with BS. This secret key is also known as the personal key ($K_p$). To strengthen the secrecy of communications done within the network and to protect the communications from external adversary, each node is assigned with a single network wide session identity (ID).

Key Generation: To enhance the confidentiality of the message communicated within the network, each and every message to be transmitted should be encrypted with a secret key. The proposed scheme uses onetime secret key and the secret key used for encryption and decryption is generated dynamically for every session. Before initiating communication with the BS, source node generates a Session secret Key ($SK_s$). This is represented by Equation (6.5).

$$SK_s = K_p || K_w^{-1}$$  \hspace{1cm} (6.5)
Where, $K_p$ represents the personal key owned by the node and $K_w^{-1}$ is the inverse of witness key. The benefit of using this mechanism for session secret key generation is to prevent the direct exposure of key to adversary. Even though a source node or a forwarding node is captured by an adversary, the session secret key will not be exposed to the adversary as the key is not predefined or shared between the communicating nodes. But the key is generated dynamically at any instant.

**6.3.3 Anonymous and Secure Communication Phase**

The proposed scheme is able to achieve anonymous and secure communication. The source node generates the event report protected by means of the session secret key. Along with the protected event information, to maintain authenticity of the report in transit two MACs (Message Authentication Code) are also enclosed. One MAC generated using the witness key $K_w$ and the other MAC generated through the session ID.

To enhance the privacy of the information in transit the proposed scheme follows the concept of anonymity. The proposed scheme focuses on a hop by hop anonymous secure communication.

In this scheme hop by hop anonymous communication is achieved by combining the address of the one hop forwarding node along with the protected event information. Each event reports combined with the destination information is represented in encrypted form is sent to the one hop forwarding node. The format of the report is represented as

$$E_{K_w}(\text{Dest}, E_{SK}(\text{Event})), \text{MAC}(E_{K_w}(\text{Event}), \text{MAC (session ID, Event}))$$
Where, ‘Event’ represents the triggered event information and ‘Dest’ represents the address of the one hop forwarding node or the address of the BS. When a forwarding node receives the report it checks whether there are two MACs endorsed along with the protected event information.

If it contains the required MAC, then extract the MACs from the report and compare with the computed MACs. If the authentication process succeeds, then it updates the report by combining the destination address of its one hop forwarding node.

Destination address along with the protected event information in encrypted form is forwarded to next hop along the path. Otherwise, if there is any failure in authentication then the report is immediately discarded. Thus the process can be chained by using the encrypted message.

Each encrypted mix of destination address along with encrypted event information is decrypted and then re-ordered before it is forwarded. When the BS receives the report it performs the authentication process endorsed in the report.

If the verification fails, then it discards the event report. The flow diagram for establishing secure communication is represented through Figure 6.3. This approach has high anonymity by hiding the real event traffic with a dummy traffic and strong security against compromised nodes involved in communication.
Encrypt the event information using Session Secret Key (SKs)

Mixes encrypted event information with address of next hop

Encrypts the mixed information using witness key (Kw) and forward to next hop

Next hop verifies the authenticity

If Authentic

Yes

Forwards the report by re-ordering the report by including the address of its next hop

No

If next hop is Base Station

Yes

Verifies the authenticity and if authentic retrieve the event information

No

Drop the report

Figure 6.3 Flow diagram for secure communication
6.4 SECURITY ANALYSIS OF THE PROPOSED SCHEME

To evaluate the effectiveness of the proposed scheme, it is necessary to investigate the attack models which threaten the proposed protocols and determining the resilient rate of the proposed scheme against passive attacks, active attacks that occur in the communication path, node capture attack and traffic analysis attack. The proposed scheme is designed to be resistant to the following attacks.

**Resilient to passive attacks during communication**: Passive attackers are able to perform eavesdropping at any point of the networks. They can guess about the future communication based on the eavesdropped messages. In the proposed scheme event information communicated contain the security features confidentiality, authentication, integrity and anonymity.

Even though adversary is able to get the encrypted event report through eavesdropping, he cannot get the key used for decrypting the encrypted report. Further, the adversary is unable to get the source information because the sender hides its identity to maintain privacy of the data. Hence it is determined that the proposed secure communication scheme has the solutions to function as countermeasure for passive attack.

**Resist certain active attack on the path of communication**: Active attackers have greater ability than passive attackers. The active attackers can forge, reply and modify messages in transit. The proposed scheme is resilient to some of the active attacks such as selective forwarding and forwarding a falsified report etc. In the proposed scheme the event information or any other information sent by a source node is forwarded through authenticated en-route nodes.
Before making changes to the packet the en-route node should receive the authentication information. It is difficult for the adversary to perform selective forwarding attack without holding route authentication information. Even though adversary is able to falsify event report, it will not be forwarded to BS. The report is forwarded only after verification of authentication information endorsed in the report.

**Effect of node compromisation:** In the proposed scheme node compromisation does not cause serious effects in communication. The adversary is unable to succeed in his actions by compromising a node. Even if an en-route node is compromised it does not produce serious effect in exposing secret information as secured information in transit cannot be revealed by the compromised node.

Authentication information or the symmetric key used for securing the event information cannot be exposed to the compromised node. Hence, it is confirmed that the data compromisation does not cause more issues in establishing secure communication through the proposed scheme.

**Resilient to traffic analysis attack:** The proposed scheme offer anonymous communication identities of the destined sensor nodes and are protected from being revealed to any other node. Moreover, by means of the proposed hop-by-hop anonymous communication encryption and decryption are done at each intermediate hop to maintain the privacy of the information in transit and different hops may produce different encrypted output and even if the encrypted information can be received by an adversary he may not be able to retrieve the original information. The strong secrecy achieved is due to the session secret key generated by the individual sensor nodes and may not be exposed to any other node.
Complexity analysis of ASDTS:

Computational overhead arises in the proposed scheme due to the operations such as generation, distribution of keys and authentication of the event report. Also in the proposed scheme neighbouring nodes establish association among them based on id-based scheme. This requires additional computation overhead. The security achieved through the proposed scheme is stronger than the related schemes LED and PESC. But proposed scheme spend more energy to compute the authentication information for each report.

6.5 SIMULATION AND RESULTS

6.5.1 Simulation Study

The proposed mechanism is evaluated by comparing the simulation results with the results obtained through related schemes. The main objective of the simulation is to evaluate the performance of the proposed secure communication scheme and its security relevant issues in the presence of compromised nodes in a WSN. A WSN of 500 nodes is randomly deployed into 1000x1000m$^2$ area of interest. All sensor nodes are assigned with unique id.

The simulation results are studied by varying the count of compromised nodes and the size of the network. This scheme is highly resilient to traffic analysis attack caused by compromised forwarding node along with the path of communication. The parameters used in simulation are tabulated in Table 6.2.
Table 6.2 Parameter settings for simulation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum nodes in the network</td>
<td>500</td>
</tr>
<tr>
<td>Initial energy of network</td>
<td>1000 joules</td>
</tr>
<tr>
<td>Number of compromised nodes</td>
<td>5 to 30</td>
</tr>
<tr>
<td>Energy for each sensor node</td>
<td>2 joules</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>50 m</td>
</tr>
<tr>
<td>Energy consumption for transmission</td>
<td>75 µJ</td>
</tr>
<tr>
<td>Energy consumption for receiving</td>
<td>80 µJ</td>
</tr>
<tr>
<td>Time consumption for hash operation</td>
<td>1.5 milliseconds</td>
</tr>
</tbody>
</table>

6.5.2 Algorithms used for Comparison

The performance of the proposed scheme is studied and analyzed by comparing with related end-to-end secure communication schemes Location-Aware End-to-End Data Security (LED) (Ren et al 2008), a fuzzy based approach for false data detection in WSNs (Lee et al 2010) and Providing End-to-End Secure Communication scheme (PESC) (Wenjun et al 2011) in terms of probability of end-to-end communication, data compromisation probability, filtering false endorsement, node capture probability and key sharing probability.

Ren et al (2008) discusses about a technique proposed to provide data security in WSNs. The authors used the location information to generate the keys. This scheme is applicable to static WSNs. The authors collect the location information of the sensor nodes after deployment using a localization scheme. The deployment area is divided into grids and each grid consists of number of cells. Three different types of keys are assigned to each sensor nodes.
This location based scheme resists the impact of compromised node on the event report generated by the neighbouring sensor node. But if a node within the cell gets compromised there may be chances for the adversary to break the confidentiality of reports. The false data detection probability of the en-route nodes in this scheme is very low.

Lee & Cho (2010) propose a Fuzzy based Detection of Injected False Data (FDIFD) in WSNs. In this scheme false data is detected by BS by means of verifying the authenticity of sensing reports. The input factors used in fuzzy logic for verifying the validity of the report are correctness of the report, the number of the report and the fluctuation in the number of the reports. Each event report under verification contains source identifier, type of the object and time stamp along with the MAC attached to the report.

Even though this mechanism is assumed to save energy, the false data detection system followed in this scheme is not energy efficient. As most of the energy of the en-route nodes and the energy of the BS is wasted if a false report is allowed to travel along the path until it reaches the BS. Further this scheme does not demand for a secured path for establishing secured communication.

Wenjun et al (2011) described a secure communication scheme to achieve end-to-end security in WSNs. In the proposed scheme authors used a technique for key pre-distribution and efficient key sharing between single hop and two hop paths. The authors divide the entire sensor network into number of classes and pre-distribute keys into classes. For key sharing nodes generate multiple key shares and each share is sent through multiple paths. Each share is encrypted and decrypted hop-by-hop.

The authors analyzed the key management of the proposed scheme and determine that the proposed scheme can achieve enhanced performance
when used along with other secure routing protocols. This scheme requires a key pre-distribution mechanism to distribute different types of keys to different classes of nodes. Further, before establishing communication, this scheme needs to determine a highly resilient path.

### 6.5.3 Results and Discussion

This section presents some of the results obtained through simulation of proposed ASDTS and the related schemes. The results refer to measures of performance efficiency and security efficiency. The metrics that are chosen to evaluate the efficiency in addition to the effectiveness of the schemes are: end-to-end data delivery rate, network lifetime, false data detection probability, probability of compromising the communication link, resilience to node capture.

Probability of end-to-end data delivery: This metric measures the probability that the BS can successfully receive data from a sensor node without being disclosed to the en-route nodes. Packet delivery ratio can be computed as ratio of the numbers of packets successfully delivered to the BS to the number of packets sent by the source along the selected path.

Probability of disclosing secret information: This metric is measured by determining the number of secret keys exposed to the adversary on compromising a node.

Probability of key connectivity: The key connectivity probability of any node is determined by the number of common keys shared between nodes to total number of keys stored in each node.
Figure 6.4 End-to-End data delivery in the presence of compromised nodes

Figure 6.4 highlights end-to-end data delivery ratio of the proposed and related schemes in the presence of compromised nodes. The proposed and the related schemes are experimented in a network of 500 nodes and when tested in the presence of 15 compromised nodes the proposed ASDTS achieves the data delivery ratio of 88%. In contrast the related schemes LED and PESC achieved the data delivery ratio of 76% and 84%.

When considering a network with 25 compromised nodes the proposed ASDTS achieves 84% of data to be delivered to BS and the related schemes LED and FDIFD ensures 70% and 75% of data to be successfully delivered to BS. The high packet delivery ratio offered by the proposed scheme is due to the resiliency against data compromisation due to anonymity and secrecy in communication. The relation between the number of compromised nodes and end-to-end data delivery ratio seems to be linear in the proposed scheme ASDTS. Because of the symmetric key used for securing the event information cannot be exposed to the compromised node.
Hence, it is confirmed that the data compromisation does not causes more changes in the data delivery ratio.

Figure 6.5 Data delivery ratio with respect to change in network size

Figure 6.5 demonstrates the end-to-end data delivery ratio achieved through the proposed and related schemes in the absence of compromised nodes. When experimented in an environment with 200 nodes the ratio of the packets delivered to the BS by ASDTS is 86%. While considering the same environment for the related schemes PESC and FDIFD the amount of packets delivered to destination are 82% and 78% and when the network size is increased to 500 nodes the ratio of packets delivered to destination through the proposed scheme is 94%. It is determined that when the network size increases the number of packets delivered to the destination gets increased. The high packet delivery ratio offered by the proposed ASDTS mechanism is due to the high connectivity maintained along the path.
Figure 6.6 Network lifetime in the presence of compromised nodes

Figure 6.6 illustrates the variation in the network lifetime with respect to the number of compromised nodes present in the network. The lifetime of the network is determined based on the energy consumed for establishing secure end-to-end communication. It is observed through simulation that the proposed scheme ensures increased network lifetime in the presence of compromised node. When there are 20 compromised nodes in a network with 500 nodes the maximum network lifetime achieved through proposed scheme is 590 seconds and through PESC is 560 seconds. In contrast the related schemes FDIFD and LED show less effectiveness maximum energy consumed in establishing secure communication. In the proposed scheme, the chance of selecting the next forwarding node in the routing path selection for secure communication depends upon the residual energy and traffic pattern. In this regard, the network lifetime of ASDTS seems to be linear with respect to the number of compromised nodes.
Figure 6.7 Probability of compromising secured data

Figure 6.7 illustrates the probability of compromising secured data in the presence of compromised nodes. The proposed scheme provides a disclosure rate of less than 0.2 in the presence of different number of compromised nodes. When experimented in a network with 500 nodes in the presence of 10 compromised the probability of disclosing secret information by the proposed ASDTS is 0.14 and in the same environment the probability of secret information disclosed through the schemes PESC and LED are 0.16 and 0.24. The reduced disclosure rate offered by the proposed scheme is due to the strong security offered by the proposed secure communication scheme. The disclosure rate of the secured data is lesser than the existing schemes and the graph of ASTDS seems to be linear. This is due to the mixing of the encrypted information with the address of the selected next hop neighbour using witness key.
Figure 6.8 False data filtering probability

Figure 6.8 compares the false data detection efficiency of four different secure communication schemes. These schemes are tested by assigning compromised nodes towards the path of data transmission and they are allowed to modify the data in transit.

When tested in the presence of 30 compromised nodes in a network of 500 nodes, it is determined by using ASDTS 80% of the false data has been detected within 2 hops and through LED and FDIFD only 67% and 76% of the false data has been detected within 2 hops. ASDTS achieved high false data filtering effect as most of the false data packets can be detected by the immediate neighbour of the compromised en-route node.
Figure 6.9  Comparison of key connectivity probability with respect to node compromisation probability

Figure 6.9 shows the relationship that exists between nodes through key sharing probability. The key connectivity probability is determined by the number of common keys shared between nodes to total number of keys stored in each node. In a network with 500 nodes in the presence of 25 compromised nodes when the node compromisation probability is 0.7 whereas the proposed scheme achieves 0.1 key connectivity probabilities.

In proposed ASDTS scheme each and every node shares a single secret key only with the BS. Hence the key connectivity probability of the proposed scheme is very low. But LED achieves the key connectivity probability of 0.34 when the node compromisation probability is 0.7. In LED each node has common keys shared with nodes belonging to a single cell and the nodes belonging to the adjacent cells of WSNs.
Figure 6.10 End-to-End data propagation delay

Figure 6.10 shows the effect of end-to-end delay caused in propagating a packet from source to BS. The longer delay occurred in the schemes LED, FDIFD is due to control and communication overhead which occurs in establishing secure end-to-end data transfer. In contrast the proposed scheme ensures shorter delay as the time consumed for exchanging control overhead is very much reduced.

It has been observed through simulation the delay caused by proposed ASDTS when there are 20 compromised nodes in a network with size 500 nodes is 20 milliseconds. But the related schemes LED and FDIFD achieve delay of 25ms and 28ms due to the exchange of control messages in achieving the security services. The delay that occurs in the proposed scheme is due to the authentication request and reply message exchanged between source and destination before initiating secure communication. Also the presence of compromised nodes increases the necessity for retransmission of data through an optimal path.
Table 6.3 Comparative analysis of ASDTS with existing schemes

<table>
<thead>
<tr>
<th>parameters</th>
<th>LED</th>
<th>FDIFD</th>
<th>PESC</th>
<th>ASDTS (proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data delivery ratio in the presence of 25 compromised nodes (percentage)</td>
<td>70</td>
<td>75</td>
<td>78</td>
<td>84</td>
</tr>
<tr>
<td>Network lifetime in the presence of 30 compromised nodes (seconds)</td>
<td>500</td>
<td>470</td>
<td>530</td>
<td>560</td>
</tr>
<tr>
<td>Probability of compromising secured data in the presence of 30 compromised nodes</td>
<td>0.4</td>
<td>0.36</td>
<td>0.25</td>
<td>0.22</td>
</tr>
<tr>
<td>False data detection rate at 8\textsuperscript{th} hop (percentage)</td>
<td>80</td>
<td>86</td>
<td>91</td>
<td>94</td>
</tr>
<tr>
<td>Key connectivity probability when node compromising probability is 0.9</td>
<td>0.32</td>
<td>0.37</td>
<td>0.48</td>
<td>0.12</td>
</tr>
<tr>
<td>End-to-End data propagation delay in the presence of 30 compromised nodes(milliseconds)</td>
<td>30</td>
<td>33</td>
<td>22</td>
<td>25</td>
</tr>
</tbody>
</table>

Table 6.3 shows the comparison of ASDTS with the existing system for different parameters. The parameters may be the filtering efficiency, packet delivery ratio, data compromisation probability, and the Network lifetime. The proposed scheme achieves high packet delivery ratio with low data compromisation probability. The existing end-to-end secure communication schemes are subjected to node compromisation due to the high key sharing probability among sensor nodes. The proposed scheme resists the malicious activities performed along the path used for communication particularly it resists the traffic analysis attacks performed by compromised en-route nodes.
The maximum performance achieved in the proposed scheme is due to selection of optimal path and the principle of anonymity during data transmission. The delay that occurs during end-to-end communication is very much reduced in the proposed mechanism.

6.6 SUMMARY OF THE CONTRIBUTIONS

This chapter presents a design of secure communication framework by means of security services anonymity, confidentiality and authenticity along with the selection of optimal path for data transmission. The proposed scheme focuses on ensuring security in timely manner without any preparation on the receiver side for key sharing. Existing schemes LED and FDIFD require pre-key sharing mechanisms and an initial setup phase to provide security association before initializing secure communication. Further, proposed scheme is able to achieve Unabsorbability, and unlinkability.

By making use of anonymity it prevents the leakage of the identity of the participants. Even though the identity of the sender is known, the adversary is unable to guess or determine the information on transit. The security features are measured in terms of probability of exposing secure information, key connectivity probability, End-to-End data delivery and false data detection probability. It is determined that false data detection probability of the proposed ASDTS is superior to other schemes LED and FDIFD due to their increased detection probability with reduced computation and communication overhead.

Further, probability of exposing secure information of ASDTS is decreased due to the minimum key sharing probability with other nodes. The proposed scheme is highly resilient to insider and outsider attacks due to the anonymous and secured communication offered.