CHAPTER 5
PAIR KEY BASED TRUST AUTHENTICATION PROTOCOL FOR AUTHENTICATION IN WIRELESS SENSOR NETWORK

5.1 ENACTMENT OF EXISTING TRUST BASED PROTOCOLS

This chapter presents a comparative study of role of trust management in various trust based protocols and further, pair key based trust authentication protocol is developed. PTAP is compared and analyzed based on security perspectives. The performance metrics of PTAP influences greater heights, due to cryptographic functions.

5.1.1 Trust Aware Routing Framework

TARF has been designed in order to avoid replay of routing information by attackers and also it is energy efficient by accepting some level of overhead. The authors mainly focus on data collection task and thus, the routing needed for data collection task is essential to report the collected data to BS. If replay of routing information is performed by attacker by creating forged identity of BS, then the fake BS receives collected data and the data are not delivered to original BS. TARF is designed based on neighbor node, its trust level and energy cost. The components such as energy watcher and trust manager are used to estimate energy cost which is then followed by route selection algorithm as discussed by Guoxing et al. (2010). This existing TARF is implemented with TinySec for authentication and encryption which utilizes 20912 bytes of ROM capacity and 1464 bytes of RAM. Further, evaluation of performance metrics is done for comparative study with the proposed scheme.
The delivery ratio is the numbers of messages received by actual BS by performing an experiment of setting a fake BS node say $N_f$. The number of packets received at original BS $N_o$ is measured and it is shown in Figure 5.1. Depending upon the number of packets received at original BS, the control overhead, which is due to delay in both control packet and data packet delivery, is measured with respect to increasing execution time. It is proved by Guoxing et al. (2010) that 60% of delivery ratio is obtained and thus, nominal overhead is reflected in Figure 5.2.

![Figure 5.1 TARF: Number of nodes vs. Delivery ratio](image1)

![Figure 5.2 TARF: Execution time vs. Control overhead](image2)
Since TARF uses energy watcher and trust manager to monitor and gather the data report, the migration of nodes due to mobility is not affected purely. Thus, TARF achieves a proper flow of network stability rate after 40 nodes as shown in Figure 5.3. But, if the mobility level is more, the energy watcher and trust manager couldn’t get the correct reports which will be reflected as linear decrease in network stability rate.

![Network Stability Rate](image1)

**Figure 5.3 TARF: Network stability rate**

![Link Reliability Rate](image2)

**Figure 5.4 TARF: Link Reliability Rate**
Link reliability rate infers to the integrity of packets delivered at destination. Number of links and reliability rate are proportional to each other in TARF. The forged identity of BS is avoided to some extent by trust manager and thus replaying if the information is reduced. Therefore, the integrity of packets is increased depending on the number of links as shown in Figure 5.4.

![Figure 5.5 TARF: End to end delay](image5.5.png)

![Figure 5.6 TARF: Network lifetime vs. Throughput](image5.6.png)
TARF measures delay depending on the performance of hop per delivery. TARF shows 50% of delay which is half midway in delivering packets to the destination. The end to end delay measured at each pause time is shown in Figure 5.5. Throughput of TARF is compared with network lifetime in Figure 5.6 in turn, the network lifetime depends on the number of nodes taken for a sample network loop. A sample of 35 nodes are taken within which any 6 nodes are not able to forward data to BS, thus 70% of throughput is achieved by TARF. Authentication rate is nominal for first few portion of execution time in Figure 5.7 during which replay of information will be highly pronounced. Once there is an increase in execution time, a slow start of authentication rate emerges.

![Figure 5.7 TARF: Authentication rate](image)

5.1.2 Trust Based Routing Scheme

The trust based routing scheme proposed by Aweek et al. (2012) is based on three tiered architecture which comprises cluster based environment. The main work of TRS is to filter out illegal nodes from the space of legal nodes based on some trust evaluation. Trust evaluation initially focuses on remaining battery level of SN. If the remaining battery level is lesser than the average remaining battery level of all the SN, the node is considered as malicious. This is
because malicious node spends much time in running unnecessary coding. Further, sensing communication is believed to be sustained for certain amount of time and if any node does not send the data packets after a specified time interval, then the node is considered as misbehaving nodes. Later, variation in sensed data is considered (i.e.) validity of data sent by SN is determined by comparing it with the value of any four nearest SN. Finally, the trust value status of sample nodes is measured. The packet delivery ratio is in decreasing status as shown in Figure 5.8. Since TRS is maintaining some specific time interval pattern which makes the cluster head to drop some packets due to unreachability, this reflects in reduced delivery ratio.

![Figure 5.8 TRS: Number of nodes vs. Delivery ratio](image)

TRS accepts the data packets only after comparing with the target sample packets of neighbor nodes and introduces delay in delivery of packets and also the battery level plays a major role in measuring the sustainability of SN. Because of this combination, the control overhead increases during execution time as in Figure 5.9. Network stability rate also decreases due to straight forward assessment of trust evaluation and it is shown in Figure 5.10. But, TRS depicts greater heights in link reliability rate, because of constrained
identification of malicious nodes, such as checking battery level, sensing communication capability and measuring the variation in sensed data. This is shown in Figure 5.11. Thus, the integrity of packets increases. The delay discussed during delivery of packets is shown in Figure 5.12.

Figure 5.9 TRS: Execution time vs. Control overhead

Figure 5.10 TRS: Network stability rate
Figure 5.13 delivers that, if more number of nodes are sustained in the network, after authenticating them, the TRS surely steps towards increasing range.

The authentication among SN is fairly pronounced in TRS as shown in Figure 5.14. This is due to the avoidance of illegal nodes from legal one based on the battery level. The misbehaving node, which is performing illegal access, depletes most of its energy by pulling down its battery level. Due to this, the measurement of power level compared with average of all SN becomes degraded. But, still any default power conservation mechanism is not best suitable for this work. Therefore, any on demand protocol will be the best fit to measure the power level.

Figure 5.11 TRS: Link reliability rate
Figure 5.12 TRS: End to end delay

Figure 5.13 TRS: Network lifetime vs. Throughput
5.1.3 Trust Guaranteed Routing

Trust management system of TGR is developed based on trust factors for which various trust factors that influence trust are analyzed by Geetha & Chandrasekaran (2014). Layer based hierarchy of trust management is developed. Moreover, the layers such as application, transport, datalink and physical layer interacting with trust management system are shown. The different trust factors such as communication trust, data trust, functionality trust, location trust and energy trust are computed. Depending on this and trust models used, the trust is calculated and updated correspondingly.

Figure 5.14 TRS: Authentication rate

Figure 5.15 TGR: Number of nodes vs. Delivery ratio
Nominal packet delivery ratio is attained, due to concentration on trust factor is more in TGR and thus, time incurred in calculating trust is considered before delivering of packets to destination. It is shown in Figure 5.15, each node forwards the packet to next node depending upon the trust value. If the trust value is not satisfied, the packets may be dropped. Correspondingly, the Figure 5.16 shows that the reduction in packet delivery reflects in more control overhead during execution.

**Figure 5.16 TGR: Execution time vs. Control overhead**

**Figure 5.17 TGR: Network stability rate**
As the number of nodes increases, the trust to be calculated for each node increases tremendously. Several trusts such as communication trust, energy trust and location trust should be calculated and it is updated in the storage space of each node. Such type of computation makes the stability of nodes to stroll downwards as in Figure 5.17. Only if all the trust values are measured noteworthy, the node becomes stable. The concentration of link reliability (i.e.) the packet integrity is concentrated much less in TGR. But, trust is reflected as a reliable path construction to destination and so, the reliability rate increases, as the network size increase. Thus, the number of links and reliability rate are directly proportional to each other which is shown in Figure 5.18.

![Figure 5.18 TGR: Link reliability rate](image)

![Figure 5.19 TGR: End to end delay](image)
Delay increases tremendously at any pause time during execution. For instance, it is incurring delay of 11.2 ms at hundredth millisecond. It is shown in Figure 5.19. This is due to the time incurred in calculating all the trust values in each node add delay in delivering packets to the destination. Further, the sustainability of network lifetime makes to have a good value of constant throughput (i.e.) if more than 85% of nodes are calculated with trust values, then the communication among SN will be reliable in establishing a higher
throughput as shown in the Figure 5.20. A better authentication rate is pronounced in TGR. Though it intakes some amount of delay in calculating trust, the nodes are authenticated, due to measurable trust values. Thus, the authentication rate increases towards execution time as shown in Figure 5.21.

### 5.1.4 Trust Aware Secure Routing Framework

Junqi et al. (2014) have discussed and analyzed various attacks such as on-off attacks, conflicting behavior, selfish attack, collusion attack that affects trust during routing in WSN. According to that, trust is computed and trust deviation schemes are pronounced. Later routing scheme with best trust metric and QoS metric is implemented. Performance metrics related to routing between SN are measured. The simulation parameter for executing TSRF is shown in Table 5.1.

**Table 5.1 Simulation parameters for TSRF**

<table>
<thead>
<tr>
<th>Parameters for execution</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution time</td>
<td>500 seconds</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Arena area</td>
<td>200 x 200 m²</td>
</tr>
<tr>
<td>Communication range</td>
<td>40 m</td>
</tr>
<tr>
<td>Interval between any two packets</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Length of data packet</td>
<td>100 bytes</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>GPSR</td>
</tr>
<tr>
<td>MAC protocol used</td>
<td>IEEE 802.15.4</td>
</tr>
<tr>
<td>Trust value considered</td>
<td>0.5</td>
</tr>
<tr>
<td>Percentage of malicious nodes (injecting fake nodes)</td>
<td>20%</td>
</tr>
</tbody>
</table>
Figure 5.22 TSRF: Number of nodes vs. Delivery ratio

Figure 5.23 TSRF: Execution time vs. Control overhead

Figure 5.22 infers that when there is minimum number of nodes say 10, packet delivery ratio is at greater height, assuming that there are no malicious nodes. If 20% of malicious nodes are injected into the network by projecting some sort of attacks, then delivery ratio decreases. Also, the path trust is 50% say 0.45, then again the delivery ratio will increase. The control overhead increases due to broadcast and rebroadcast, and thus, heavy transmission control signals arise. If some limited nodes are restricted in flooding process, the control
overhead will be in nominal range. It is shown in Figure 5.23 that during 30 to 40 seconds, the overhead remains same during restricted flooding activity. As the number of nodes increases, it is necessary to apply QoS metric and trust deviation procedure in a large factor. Thus, the increase in nodes shown in Figure 5.24 makes the stability rate to decrease.

**Figure 5.24** TSRF: Network stability rate

**Figure 5.25** TSRF: Link reliability rate
Packet integrity is measured via link reliability. It is increased and shows betterment, when there is an increase in number of links as shown in Figure 5.25. Since trust deviation procedure and QoS metric are satisfied for links established between SN, the number of links and the link reliability rate are directly proportional to each other. The end to end delay also covers the time spent on route establishment. When flooding is limited to 2 hop limit, TSRF saves 32.2% of time. This is achieved during when average number of neighbor nodes is equal to 14. Approximately, 70% of latency is covered in TSRF and thus, the Figure 5.26 shows an increase in delay at any pause time during execution.

![Graph showing end to end delay](image)

**Figure 5.26 TSRF: End to end delay**

Figure 5.27 shows the measurement of throughput versus network lifetime where the throughput is considered with number of packet transmitted between SN. Throughput reaches 79% at a point of 160 seconds, when the neighbor nodes are in the range of 14. But, during 20 seconds, the neighboring nodes are more and thus, needs to calculate trust for more number of nodes. It restricts the percentage of throughput.
Authentication rate depends on the trust value computed with respect to neighbor nodes. Authentication rate grows rapidly, when the trust value is computed during lack of deviating behavior but, if the malicious node introduces on-off attack, the authentication rate will decreases. This scenario is shown in Figure 5.28.
5.2 SECURITY ANALYSIS OF EXISTING TRUST MANAGEMENT SYSTEM

The existing schemes considered for comparative study of trust based work are TARF, TGR, TSRF and TRS. All the four schemes discussed are pronounced with trust compatibility with WSN. Every scheme has analyzed the security impact in terms of calculating trust values. The stability of nodes is measured by injecting fake nodes to characterize different attack scenarios. The same scenario of existing schemes has been tried in NS2 simulator to achieve the performance metrics. All the performance metrics that are needed to compare with the proposed scheme is measured. Among the four trust management schemes, TSRF stands first, since it focuses on avoiding replay of routing information. TGR is developed with many trust factors and it enables to avoid malicious node in good percent. The performances of TARF and TRS are moreover equivalent, even though both have different scenarios of focus in calculating trust.

5.3 PROBLEM FORMULATION FOR EFFICIENT TRUST AUTHENTICATION IN WSN

The trust management scheme discussed so far has not concentrated on security strength of key generation between SN. Compromising of nodes is discussed but the way point of compromised keys which destroys legitimate nodes, is not focused. Thus, the trusted authentication and cryptographic operations should be integrated to provide best non-compromising scenario and this becomes the objective function for developing pair key based trust authentication protocol.
5.4 PAIR KEY BASED TRUST AUTHENTICATION PROTOCOL (PTAP)

The overall data flow diagram of pair key based trust authentication protocol is shown in the Figure 5.29 which depicts the modules performed in this chapter. The major symbols used in PTAP is mentioned in the Table 5.2.

![Data flow diagram for PTAP](image)

**Figure 5.29 Data flow diagram for PTAP**

5.4.1 Threshold Based Identification of Legitimate Nodes

In WSN, trust is defined as the relationship between trusting nodes and trusted nodes. This trust relationship is determined by rules to evaluate the evidence with a quantitative way which is generated by the previous behaviors...
of nodes. The proposed authentication protocol consists of trust assessment method, key generation approach, encryption and decryption concept in which the key generation process gets the input from DKO. By doing this, the pairwise key generated by DKO is optimized to higher secure level by introducing authentication and integrity among nodes.

Table 5.2 Description of symbols used in PTAP

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varsigma$</td>
<td>Period</td>
</tr>
<tr>
<td>$\tau$</td>
<td>Delay received packets</td>
</tr>
<tr>
<td>PAR</td>
<td>Packet Arrival Rate</td>
</tr>
<tr>
<td>PFR</td>
<td>Packet Forwarding Rate</td>
</tr>
<tr>
<td>RF</td>
<td>Reliability Factor</td>
</tr>
<tr>
<td>$R^{A}_{B}$</td>
<td>Node Recommendations</td>
</tr>
<tr>
<td>$\mathbb{V}</td>
<td>A \rightarrow B</td>
</tr>
<tr>
<td>$KAT$ and $KBT$</td>
<td>Symmetric keys</td>
</tr>
</tbody>
</table>

The subject determines the trust values of objects according to both straight and circuitous trust values. Assume the node $k$ is subject, which not only makes straight assessment of object $l$, but also makes circuitous estimation of object $l$ through nodes $k_1, k_2$ and $k_3$. It is assumed that node $k$ makes trust estimation for node $l$ and adopts acknowledgement mechanism. In this case, trust threshold value is maintained to find the malicious node. If any node falls below the trust threshold value, it is considered as misbehaving node. The trust threshold value includes packet arrival rate, packet sending rate, packet forwarding rate, reliability factor, node recommendation and node proposal. The determination of the above packets is given below.
Step 1:

The packet arrival rate can be calculated as ratio of common ACK packets sent to total data packets. According to the change of the rate, it is known that the node $k$ has response counterfeit behavior. If the change maintains in the interval $(-\xi_1, \xi_2)$ in different periods, node $k$ works normally. Packet Arrival Rate $PAR_{a,b}(\tau)$ represents the number of received packets,

$$PAR_{a,b}(\tau) = \frac{PA_{a,b}(\tau)-PA_{a,b}(\tau-1)}{PA_{a,b}(\tau)+PA_{a,b}(\tau-1)}$$  \hspace{1cm} (5.1)

Step 2:

Let consider that $b$ sends packets to $c$ which is beyond the communication scope of $a$. If node $a$ cannot monitor the successfully sent packets rate of $b$ directly in this situation, node $a$ can monitor the number of the same packets sent by itself. It’s known that every packet sent by nodes contains a time stamp and can be renowned efficiently, even if the packets have the same content. The number of packets received at the destination is determined according to the different time stamps. $PS_{a,b}(\tau)$ is the requiring number of sent packets, and $PR_{a,b}(\tau)$ is the repeating number of sent packets. The equation as follows,

$$PSR_{a,b}(\tau) = \frac{PS_{a,b}(\tau)}{PS_{a,b}(\tau)+PR_{a,b}(\tau)}$$  \hspace{1cm} (5.2)

Step 3:

If node $p$ is beyond the communication range of node $q$, it cannot monitor the number of packets received by node $p$ directly. It is needed to collect the feedback information of node $p$ to obtain the number of received packets. In order to distinguish the forwarding packets and the remained packets, an UPDATE packet, which contains a special bit, is constructed. If any node $p$ receives a forwarding packet, it broadcasts an UPDATE packet. Then, node $q$
can collect these UPDATE packets of node \( p \) to obtain the number of forwarding packets. According to the change rate of \( PFR_{p,q}(\tau) \), it can efficiently avoid active and passive attacks, as well as identify whether the node is selfish.

\[
PFR_{p,q}(\tau) = \frac{P_{F_{p,q}}(\tau) - P_{F_{p,q}}(\tau-1)}{P_{F_{p,q}}(\tau) + P_{F_{p,q}}(\tau-1)}
\]

(5.3)

**Step 4:**

The reliability factor is introduced to prevent misbehaving nodes from modifying primary data packets. Node \( p \) acquires a packet transmitted by \( q \) randomly and makes the comparison with its own data. If the source node of this packet is in the same area of node \( q \) and the diversity rate is maintained in the interval \((-\zeta_1, \zeta_2)\), the number of accordant packets rises. Elsewise, if the source node does not belong to the area of node \( p \), the reliability factor between node \( p \) and node \( q \) will not be adopted. \( AP_{p,q}(\tau) \) is the number of accordant packets and \( IP_{p,q}(\tau) \) is the incompatible one. The Reliability factor \( RF_{p,q}(\tau) \) is as follows.

\[
RF_{a,b}(\tau) = \frac{AP_{a,b}(\tau)}{IP_{a,b}(\tau) + AP_{a,b}(\tau)}
\]

(5.4)

**Step 5:**

Evaluating the recommendation is given by \( R_B^A \) which is node A’s evaluation to node B by collecting recommendations

\[
R_B^A = \frac{\sum_{\gamma \in \gamma} |V|A \rightarrow C|\rightarrow v|C \rightarrow B|}{|V|A \rightarrow C|}
\]

(5.5)

Where, \( \gamma \) is a group of recommenders; \( V|A \rightarrow C| \) is trust vector of node A to C; \( V|C \rightarrow B| \) is trust vector of node C to B.
Step 6:

Probability that the data packets received can be defined by,

\[ P_B^A = (1 - P_{A,B}) \times (1 - P_{B,A}) \]  \hspace{1cm} (5.6)

\( P_{A,B} \) is packet loss probability from node A to node B, while, \( P_{B,A} \) is packet loss probability from node B to node A.

Step 7:

Trust Threshold value is determined based on the inclusion of packet arrival rate, packet sending rate, packet forwarding rate, reliability factor, node recommendation etc. For a node \( n_k \), if \( T V_k < T V_{thr} \), where \( T V_{thr} \) is the trust threshold vector value, the node is considered and marked as misbehaving node. If the source does not get the RREP packet or RERR packet for atleast t seconds, it will be considered as a node failure or link failure. Then, the discovery process is initiated by the source again. The same procedure is repeated by either considering lack of misbehaving nodes or with least number of misbehaving node, for the completion of reliable process.

5.4.2 Secret Pairwise Key Generation

Step 8:

Once the malicious nodes are identified and legitimate nodes are authenticated each other successfully, the key generation phase begins. During this phase, the source node sends one of its secret communication codes, randomly selected from key pool. The source node also selects randomly another secret communication code from its pool and sends it to the corresponding source node. After the reception of this secret code by the source sensor node, both have the same SCC1 and SCC2. Now, the Source node and the Forwarding Node (FN) use SCC1, SCC2, Scalar Product of Mobile Sensor Node (SPMSNj) and Scalar Product of Fixed Sensor Node (SPFSN) to generate secret key using
standard approach defined. The proposed PTAP consists of two keys i.e. Secret key and Session key both forming the pairwise key generated by DKO. It is needed to determine malicious node detection and protect the network with secure key establishment process.

Once a secret key is established between the Trust Source Node (TSN) and each sensor node, the TSN assigns a Mutual Secret Code (MSC) to its all member TSNs which is the common key among one group of members. This shared secret code is updated both periodically, when a sensor node compromising is detected. Since the sensor nodes move in the network to achieve their duties, they may need to establish a secure communication link also with neighboring sensor nodes, possibly very frequently, due to their movement within the network.

In order to keep the track of their neighboring sensor nodes, each node broadcasts a short range Hello message to know about its neighboring MNs. To establish a pairwise secret key with a neighboring sensor node, both sensor nodes will share their secret communication code IDs assigned and MSC received from key pool. Now both the sensor nodes will find the maximum number of shared codes with one another and will generate a pairwise secret key put together in MSC. The message routing is done by AODV protocol which has default specification in NS2.

\[
session_key = \prod_{d=1}^{\theta} SCCR_{1d} \mod MSC
\]  \hspace{1cm} (5.7)

Where \( SCCR_{1d} \) is a session key and MSC is a pairwise key.

**Step 9:**

Trusted node B interacts with trusted server T which acts as MS and node A and establishes the fresh mutual secret K between A and B.
5.4.3 Encryption and Decryption Model

Step 10:

E is a symmetric encryption algorithm. E can be DES, Triple DES, RC2 etc. k is a common session key that server T generates for A and B to share. \( N_A \) and \( N_B \) are nonce chosen by A and B, respectively, to allow verification of key freshness to detect replay attack. M is a second nonce selected by A which helps as a transaction identifier.

Step 11:

T shares symmetric keys KAT and KBT with A, B, respectively.

Step 12:

A encrypts data for the server containing two nonce, \( N_A \) and M, and the identities of itself and the party B to whom it needs the server to allocate a key. A sends this and some plaintext to B in message.

\[
A \rightarrow B: M, A, B, E_{KAT}(N_A, M, A, B) \quad (5.8)
\]

Step 13:

B creates its own nonce \( N_B \) and an analogous encrypted message (with the same M), and sends this along with A’s message to T in message (2).

\[
B \rightarrow T: M, A, B, E_{KAT}(N_A, M, A, B), E_{KBT}(N_B, M, A, B) \quad (5.9)
\]

Step 14:

T uses the clear text identifiers in message (2) to retrieve KAT and KBT, then verifies the clear text \((M, A, B)\) matches that recovered upon decrypting both parts of message. Verifying M in particular confirms the encrypted parts are linked. If so, T inserts a new key k and the corresponding nonce into distinct messages encrypted for A and B, and sends both to B in message (10).

\[
T \rightarrow B: E_{KAT}(N_A, K), E_{KBT}(N_B, K) \quad (5.10)
\]
Step 15: 

B decrypts the second part of message (3), checks $N_B$ matches that sent in message, and if so passes the first part on to A in message.

$$B \rightarrow A: E_{K_{AT}}(N_A, K) \quad (5.11)$$

Step 16: 

A decrypts message and checks $N_A$ matches that sent in message.

Step 17: 

If all checks pass, each of A and B are assured that k is fresh (due to their respective nonce), and trust that the other party T shared k with is the party bound to their nonce in message (9).

5.4.4 Performance Evaluation

Based on simulation performance, the proposed system can withstand the chosen tampering attack, black hole attack, and sybil and identity replication attacks when compared with the existing trust management schemes. The security analysis of existing schemes is discussed in section 5.2. Since the security analytical model was not proved for attackers in the previous work, PTAP step towards in analyzing the performance of network by injecting the above said attacks during simulation. The detail security analysis of PTAP is pronounced in the section 5.5.

5.4.4.1 Simulation model and parameters

The proposed pair key based authentication protocol is simulated with Network Simulator tool (NS 2.34). In the simulation, 100 sensor nodes move in a 1300 x 1300 m$^2$ region for 100 seconds simulation time. It is assumed that each node moves autonomously with the same average speed. All nodes have the same transmission range of 200 meters. The simulated traffic is Constant Bit
Rate (CBR). The simulation settings and parameters are summarized in Table 5.3.

<table>
<thead>
<tr>
<th>Table 5.3 Simulation settings and parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes</td>
</tr>
<tr>
<td>Area Size</td>
</tr>
<tr>
<td>Mac</td>
</tr>
<tr>
<td>Radio Range</td>
</tr>
<tr>
<td>Simulation Time</td>
</tr>
<tr>
<td>Traffic Source</td>
</tr>
<tr>
<td>Packet Size</td>
</tr>
<tr>
<td>Mobility Model</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

5.4.4.2 Performance metrics

Evaluate mainly the performance results according to the following metrics.

**Average end-to-end delay:** The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

**Average Packet Delivery Ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

**Network Lifetime:** It is defined as the number of epochs delivered to destination based on node battery.

**Network Stability Rate:** Number of nodes are stable during high mobility environment.

**Link Reliability Rate:** Packet integrity is maintained through the links to destination.

**Control Overhead:** Ratio of control packets to the data packets received.
The simulation results are presented in the next part. The comparison of proposed protocol PTAP with Trust-Aware Routing Framework (TARF), Trust Based Routing Scheme (TRS), Trust Guaranteed Routing (TGR) and Trust-Aware Secure Routing Framework (TSRF) in presence of random mobility environment is presented.

5.5 RESULTS AND DISCUSSION

Nodes actual behaviors comply with the Bernoulli trial, which means that the probability that a node performances, worthy, is predetermined. If a node acts well for less than 30 percent of the interactions, it is considered as a malicious node. By default, the malicious node in the network is 10 percent.

In the first experiment, the no. of malicious nodes is varied depending upon the attacks injected. Figure 5.30 shows the results of delivery ratio for the nodes utilizing pairwise key scenarios. Clearly, the proposed scheme achieves more delivery rate than the previous schemes. The proposed scheme contains trust node estimation method to identify legitimate nodes and forwards the packets through the nodes. Hence the packet delivered at the destination is more.

![Figure 5.30 Comparison of delivery ratio](image-url)
Figure 5.31 Comparison of control overhead

Figure 5.31 shows the results of Control overhead versus Time. From the results, the proposed authentication protocol achieves less overhead than the previous schemes. It is because of the key generation process. The complexity of key is very less to achieve minimum overhead.

Figure 5.32 Comparison of network stability rate

Figure 5.32 shows the results of network stability rate for the 100 node scenarios. Clearly, the proposed system achieves more stability rate than previous trust management systems. The proposed system comprises two major aspects i.e. trust node evaluation and encryption process. Packet is delivered via
reliable nodes through stable link. Figure 5.33 shows the results of Link Reliability Rate versus No. of Links. From the results, it is clear that the proposed protocol achieves high reliability rate than the previous systems. Link reliability is calculated based on reliability factor of trust evaluation. Figure 5.34 shows the results of end to end delay versus Pause time. From the results, it is understood that the proposed protocol achieves less delay than the previous systems because of channel quality and reliable link selection.
Figure 5.35 Comparison of network lifetime vs. Throughput

Figure 5.35 shows the results of Network Lifetime versus Throughput. From the results, it is inferred that the proposed system has high network lifetime than the previous systems. The proposed system increases lifetime by number of epochs to link.

Figure 5.36 Comparison of authentication rate
Figure 5.36 shows the results of Authentication Rate vs. Time. From the results, it is seen that the proposed system has high authentication rate than previous systems. The proposed system increases authentication by means of pairwise keys.

Table 5.4 illustrates the performance of the proposed scheme achieves better in terms of QoS metrics and proposed metrics than the existing schemes.

### Table 5.4 Performance analysis of proposed and existing scheme

<table>
<thead>
<tr>
<th>Metrics</th>
<th>TRS</th>
<th>TARF</th>
<th>TGR</th>
<th>TSRF</th>
<th>PTAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Reliability Rate (links/sec)</td>
<td>10-189</td>
<td>15-141</td>
<td>16-213</td>
<td>17-221</td>
<td>18-231</td>
</tr>
<tr>
<td>Control Overhead (Packets)</td>
<td>15.6-34.5</td>
<td>13.1-32.1</td>
<td>12.3-29.5</td>
<td>11.8-25.6</td>
<td>10.8-23.8</td>
</tr>
<tr>
<td>End to end delay (msec)</td>
<td>5.6-14.5</td>
<td>5.1-13.1</td>
<td>4.3-11.5</td>
<td>4.1-10.6</td>
<td>3.8-8.3</td>
</tr>
<tr>
<td>Network Lifetime (msec)</td>
<td>6-134</td>
<td>11-141</td>
<td>17-151</td>
<td>16-157</td>
<td>18-164</td>
</tr>
<tr>
<td>Packet Delivery Ratio(%)</td>
<td>58-21</td>
<td>65-28</td>
<td>78-34</td>
<td>81-41</td>
<td>87-56</td>
</tr>
<tr>
<td>Network Stability Rate (nodes/sec)</td>
<td>45-9</td>
<td>58-11</td>
<td>68-15</td>
<td>76-18</td>
<td>79-28</td>
</tr>
<tr>
<td>Authentication Rate (Nodes/Sec)</td>
<td>6-139</td>
<td>15-134</td>
<td>17-232</td>
<td>15-201</td>
<td>34-294</td>
</tr>
</tbody>
</table>

#### 5.5.1 Security Analysis Of PTAP

In the Figure 5.37, the survival of four different active attacks is shown for each trust management scheme. Since this thesis mainly focuses on cryptographic operations and due to integration of pairwise key generation of DKO with PTAP, security reaches prominent heights. The security analysis of existing schemes discussed in the section 5.2 concentrates on the performance based on the number of nodes compromised. But, it is essential to focus on key generation process to have efficient trusted communication among SN. (i.e.)
when a key is compromised, there is a chance of compromising both communicating parties and thus, the key must be more secure. One such secured pairwise key generated by DKO in chapter 3 is utilized by PTAP. The Figure 5.37 infers that PTAP results in lower percentage of key compromising compared to other schemes. This is achieved by simulating all the five schemes inclusive of PTAP in NS2 simulator with 100 node scenario. Since the existing scheme doesn’t infer any key generation process, the experiment is carried out with the combination of trust based routing and q-composite key predistribution. PTAP is simulated with DKO as discussed under section 5.3.

Table 5.5 Number of legitimate nodes remaining after attack execution

<table>
<thead>
<tr>
<th>Attacks</th>
<th>PTAP</th>
<th>TSRF</th>
<th>TGR</th>
<th>TARF</th>
<th>TRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybil Attack</td>
<td>94</td>
<td>80</td>
<td>90</td>
<td>81</td>
<td>90</td>
</tr>
<tr>
<td>Tampering</td>
<td>88</td>
<td>72</td>
<td>75</td>
<td>69</td>
<td>67</td>
</tr>
<tr>
<td>Black Hole</td>
<td>92</td>
<td>93</td>
<td>78</td>
<td>72</td>
<td>74</td>
</tr>
<tr>
<td>Identity Replication</td>
<td>95</td>
<td>77</td>
<td>92</td>
<td>84</td>
<td>94</td>
</tr>
</tbody>
</table>

Figure 5.37 Survival of attacks in trust management schemes
Four different active attacks are chosen namely Sybil attack, tampering, black hole attack and identity replication attacks which have major impact on WSN. These attacks should be avoided for best trust based system. Tampering makes physical disturbances to SN, Sybil attack makes multiple false identity, black hole attack will inject false routing information and identity replication attack will clone nodes with same identity within different parts of the network. These attack scenarios are falsely created by injecting fake nodes inside the network during simulation by which the performances of the protocols are analyzed. Moreover, the remaining legitimate nodes are measured during the simulation from 100 seconds to 120 seconds. The attacks injected and the legitimate nodes are shown in Table 5.5. The Figure 5.37 is graphically plotted by referencing Table 5.5.

5.6 SUMMARY OF PTAP

Trust based authentication is developed using PTAP. Performance metrics are measured and compared with four different trust based protocols. Four attack scenarios are implemented and based on that, the remaining legitimate nodes are measured. The remaining legitimate nodes are sustained based on the percentage of compromised keys.