# Analysis of Attack Scenarios in Trust Authentication Protocols

**Raghini Mohan, Miruna Joe Amali Suthanthira Amalraj, Brindha Subburaj**

***Abstract—The inducing popularity of Wireless Sensor Network (WSN) is more concern with security factors. Secure communication is essential for demanding applications of WSN. Authentication being the crucial service due to deployment of nodes in unattended environment, this paper focus on analysis of popular trust authentication protocols such Trust Aware Routing Framework (TARF), Trust Aware Secure Routing Framework (TSRF), Trust Based Routing Scheme (TRS), Trust Guaranteed Routing (TGR) and Pair Key Based Trust Authentication Protocol (PTAP). Their performance is measured in sample simulation environment. To ensure perfect security in terms of authentication service, analysis of attack scenarios are performed. To implement this, fake attacks are created and the remaining number of legitimate nodes is measured in presence of attacks such as Sybil, black hole, replication and tampering. The analysis results in showing how each protocol withstand with different attack scenarios.***

***Index Terms—Attack, Authentication, Trust, Wireless Sensor Network, Legitimate nodes.***

## I. INTRODUCTION

The emerging arena of sensor network consists of low cost sensor nodes [2-3] [5]. Such sensor environment is urgently in need of secure infrastructure. The unattended environment must provide secure interaction among Sensor Nodes (SNs) [7-8]. Thus it is essential to discuss about obstacles, requirements, major attacks and defensive measures in WSN. Before viewing the obstacles, it is essential to discuss about constraints of WSN. Resource constraints of sensor network are compact memory storage, power limitations, etc. The memory space is addressed by reducing the code size of cryptographic algorithms [1]. The miniature of SN makes the power consumption through a battery in a less percentage. The next level of obstacle is latency which is incurred during the communication among SNs. Due to network congestion and delayed routing among SN, latency increases gradually. Attacks imposing on SN are a major level of obstacles in WSN [12], [14], [18]. Various types of attacks influence different activities of WSN in a negative ground. Many trust management protocols have been arrived in order to create legitimate WSN. But it is not clearly stated that, how these cryptographic attacks are avoided.

**Role of Trust Management:** Various researches are focusing on the availability scenario of WSN to perform difficult applications [10]. Military application is one among to face various attacks. Some of the attacks may be passive eavesdropping, intrusions, flooding attacks etc. The attacks may alter information or insert fake messages in sensor network. These attacks violate the common security services such as confidentiality, integrity, authorization and authentication [6]. Cryptographic protocols without trust component cannot be applied in order to recover the attack. Here, it pictures out the need of trust component [4]. The role of trust component is to find the malicious nodes and form an environment comprising of legitimate nodes. The trust management adopted for adhoc network which is based on previous behavior is not well suited for resource constrained WSN.

Basically, many routing protocols which have been developed are based on calculating the direct trust [9] and indirect trust [15]. Some algorithms have trust based on the neighbor recommendations. Thus, WSN environment is in need of trusted authenticity which can tolerate some level of attack scenario. This paper focuses on various trust authentication protocols with its performance and analysis of attack scenarios. The analysis aims to predict the remaining number of legitimate nodes in presence of attacks under different trusted authentication protocol.

## II. TRUST AUTHENTICATION PROTOCOLS

Fenye et al. [21] developed a hierarchical dynamic trust management protocol established for cluster-based wireless sensor networks. It is based on two features such as QoS and social trust. The performance of the protocol is analyzed by using stochastic petri nets techniques and objective trust obtained based on ground truth node status. The protocol is validated by considering the objective trust with subjective trust attained during execution. This hierarchical trust management protocol can be applied to trust-based geographic routing and trust-based intrusion detection. For each application, the best trust composition and formation are calculated to maximize the application performance.

Theodore et al. [22] introduced the implementation of a location- based trust-aware routing solution named as Ambient Trust Sensor Routing (ATSR). It incorporates a distributed trust model which is based on direct and indirect trust information to defend WSN from a wide set of common routing and trust-related attacks. It is also discussed that the process

Revised Manuscript Received on December 16, 2019.

**Raghini Mohan***, Department of Computer Science & Engineering, K. L. N. College of Engineering, Pottapalayam, Tamilnadu, India,raghiragh@gmail.com

**Miruna Joe Amali Suthanthira Amalraj**, Department of Computer Science & Engineering, K. L. N. College of Engineering, Pottapalayam, Tamilnadu,India,joe.miruna@gmail.com

**Brindha Subburaj**, Department of Computer Science & Engineering, K. L. N. College of Engineering, Pottapalayam, Tamilnadu,India,brindha1963@gmail.com

learned through the design and implementation methods is used to improve the performance with the implementation cost. This target is to review that the node resources are necessary for understanding trust models and act as guiding principle for potential designers and implementers of trust models. Even though ATSR focuses on calculating both direct trust and indirect trust, the routing decisions are based on distance between SN and BS. It incorporates the broadcast message called beacon signals which will periodically announce the location information such as location coordinates node id, residual energy, reputation request message and reputation response message. Request is a multicast message indicating the gathered trust information with the neighbors and reputation response message is a unicast one which provides indirect trust information. The direct trust is computed by considering the trust metrics such as packet forwarding, network layer acknowledgement, packet precision, authentication, reputation response, reputation validation and residual energy.

Trust Aware Routing Framework (TARF) [11] protocol is mainly suitable for multihop routing environment. This framework avoids adversaries misdirecting the traffic. Base Station (BS) will broadcast periodic information about the underlined packets for the past few periods. The node which receives the periodic information will know about the new synchronization periods. TARF enforces two entities namely energy watchdog and trust manager. Energy watchdog generates cost report based on energy consumption within a period. Trust manager maintains trust level entries within the neighborhood. TARF is designed to avoid replay of routing information. If replay of routing information is performed by attacker by creating forged identity of BS, then the fake BS will receive the collected authorized data. TARF is implemented with TINYSEC which enforces encryption and authentication.

Trust Aware Secure Routing Framework (TSRF) [16] which was designed to avoid different attacks. Trust derivation and trust computation schemes are introduced in order to resist specific attacks. The author has analyzed some attacks such as black hole, grey hole, sink hole, worm hole, Sybil and DOS etc. The analyzed results made to design trust aware routing in WSN. Routing is constructed with best trust metrics and later QOS metrics are analyzed and implemented.

Trust Based Routing Scheme (TRS) [13] works on three tiered architecture. It forms a cluster based environment which helps to identify the malicious nodes from the pool of sensor nodes. The trust evaluation on sensor node is based on the remaining battery level. If the remaining battery level of a SN is less than the average battery level of all SNs, then it is considered as malicious node. Another trust evaluation is based on the validity of sensed data. The validity of data sent by SN is calculated by comparing it with nearby nodes. Finally, the trust value status is updated.

Trust Guaranteed Routing (TGR) [17] is based on several trust factors. Layer based hierarchy of trust management is developed. Moreover, the layers such as application, transport, datalink and physical layer interacting with trust management system is studied. The trust factors are communication trust, data trust, functionality trust, location trust and energy trust are calculated. Depending on this and trust models used, the trust is calculated and updated correspondingly.

Pair Key Based Trust Authentication Protocol (PTAP) proposed in [19] consists of trust assessment method, key generation approach, encryption and decryption concept in which the key generation process gets the input from Dual Key Optimization (DKO). By doing this, the pairwise key generated by DKO is optimized to higher secure level by introducing authentication and integrity among nodes. The subject $k$ determines the trust values of object 1 by both straight and circuitous trust assessments through nodes $k_1, k_2$ $and$ $k_3$. The malicious nodes are identified by trust estimation which is based on a threshold value. A trust threshold value is fixed and any node which falls below the threshold is considered as malicious node. The trust threshold value includes packet arrival rate, packet sending rate, packet forwarding rate, reliability factor, node recommendation and node proposal.

**Step 1:**

The packet arrival rate can be calculated as ratio of common ACK packets sent to total data packets..Packet Arrival Rate $PAR_{a,b}(\tau)$ represents the number of received packets,

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

**Step 2:**

The packet sending rate $PSR_{a,b}(\tau)$is calculated based on number of packets sent by a node.$PS_{a,b}(\tau)$is the requiring number of sent packets, and$PR_{a,b}(\tau)$is the repeating number of sent packets. The equation as follows,

$$PSR_{a,b}(\tau) = \frac{PS_{a,b}(\tau)}{PS_{a,b}(\tau) + PR_{a,b}(\tau)} \qquad (2)$$

**Step 3:**

The node $q$ can collect the 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.

$$PFR_{p,q}(\tau) = \frac{PF_{p,q}(\tau) - PF_{p,q}(\tau-1)}{PF_{p,q}(\tau) + PF_{p,q}(\tau-1)} \qquad (3)$$

**Step 4:**

The reliability factor is introduced to prevent misbehaving nodes from modifying primary data packets. $AP_{p,q}(\tau)$ 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.

$$RF_{a,b}(\tau) = \frac{AP_{a,b}(\tau)}{IP_{a,b}(\tau) + AP_{a,b}(\tau)} \qquad (4)$$

**Step 5:**

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

$$R_B^A = \frac{\sum_{v \in \gamma} v|A \rightarrow C| \cdot v|C \rightarrow B|}{v|A \rightarrow C|} \qquad (5)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Where,$\gamma$ is a group of recommenders; $V|A \to C|$ is trust vector of node A to C; $V|C \to B|$ is trust vector of node C to B.

**Step 6:**

Probability that the data packets received can be defined by,

$$P_B^A = (1 - P_{A,B}) \times (1 - P_{B,A}) \qquad (6)$$

$P_{A,B}$ 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 $TV_k < TV_{thr}$, where $TV_{thr}$ is the trust threshold vector value, the node is considered and marked as misbehaving node.

**Step 8: Secret Pairwise Key Generation**

PTAP consists of two keys i.e. Secret key and Session key both forming the pairwise key generated by Dual Key Optimization (DKO) [20]. 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. 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.

$$session\_key = \prod_{d=1}^{g} SCC_{1d} mod MSC \qquad (7)$$

Where $SCC_{1d}$a session key and MSC is 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.

**Step 10: Encryption and Decryption Model**

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.T shares symmetric keys KAT and KBT with A, B, respectively. The following communication instances describe the encryption and decryption process.

$$A \to B: M, A, B, E_{KAT}(N_A, M, A, B) \qquad (8)$$

$$B \to T: M, A, B, E_{KAT}(N_A, M, A, B), E_{KBT}(N_B, M, A, B) \qquad (9)$$

$$T \to B: E_{KAT}(N_A, K), E_{KBT}(N_B, K) \qquad (10)$$

$$B \to A: E_{KAT}(N_A, K) \qquad (11)$$

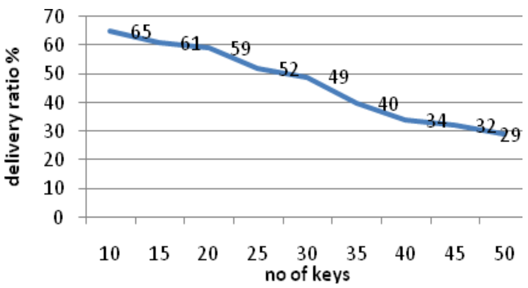
## III. Performance Evaluation of Trust Authentication Protocols

**TARF**

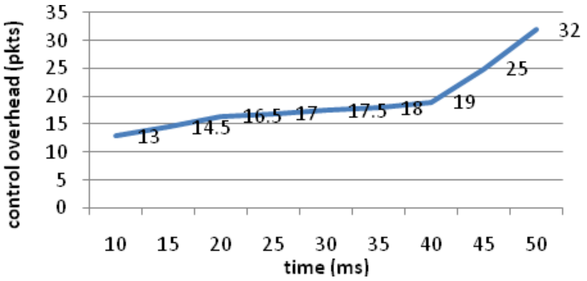
The delivery ratio is the numbers of messages received by actual BS by performing an experiment of setting a fake BS node say $N_f$ .The number of packets received at original BS $N_o$ is measured and it is shown in Figure 1(a). Depending upon the number of packets received at original BS, the control 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 in [11] that 60% of delivery ratio is obtained and thus, nominal overhead is reflected in Figure 1(b).

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 1(c). 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. 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 extend 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 1(d).

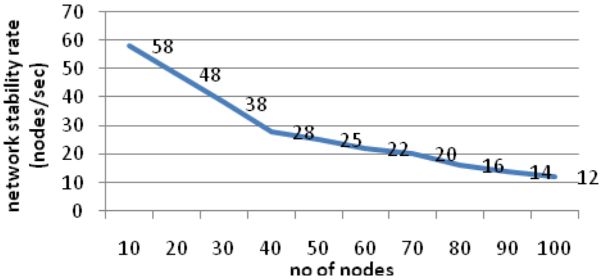
TARF measures delay depending on the performance of hop per delivery. TARF shows 50% of delay which is half midway in delivering packets to the destination. The end to end delay measured at each pause time is shown in Figure 1(e). Throughput of TARF is compared with network lifetime in Figure 1(f) in 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 1(g) during which replay of information will be highly pronounced. Once there is an increase in execution time, a slow start of authentication rate emerges.



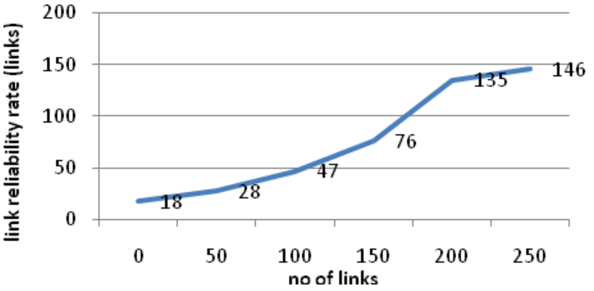
(a)



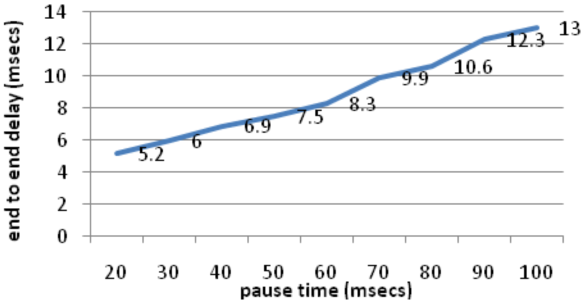
(b)



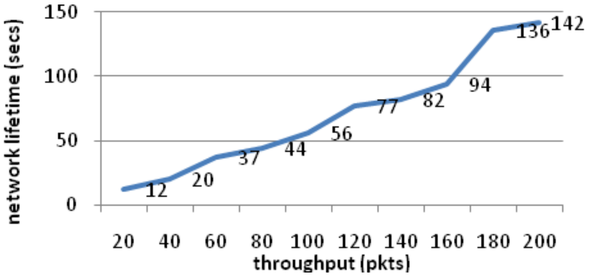
(c)



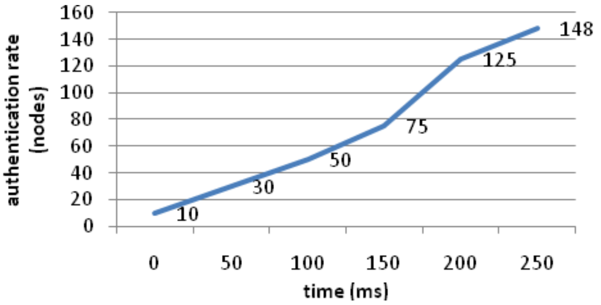
(d)



(e)



(f)



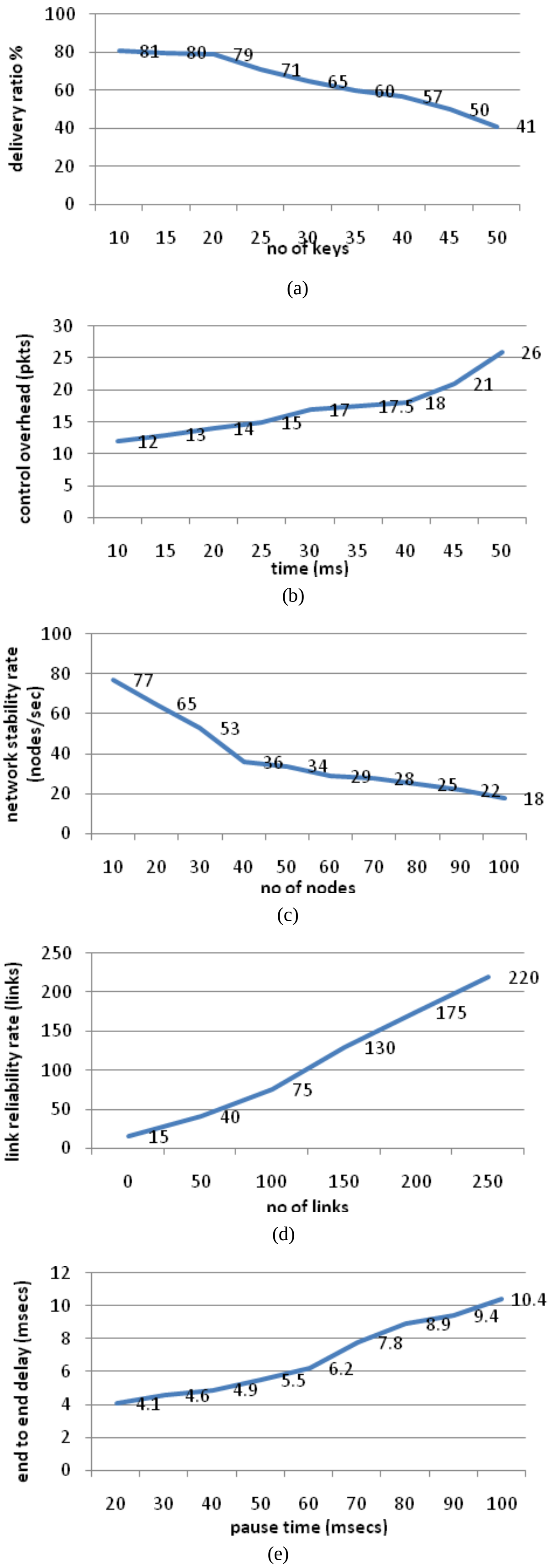
(g)

Figure 1. Performance measures of TARF

## TSRF

Figure 2(a) 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 2(b) 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 2(c) makes the stability rate to decrease.

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 2(d). 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 2(e) shows an increase in delay at any pause time during execution. Figure 2(f) 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 2(g).



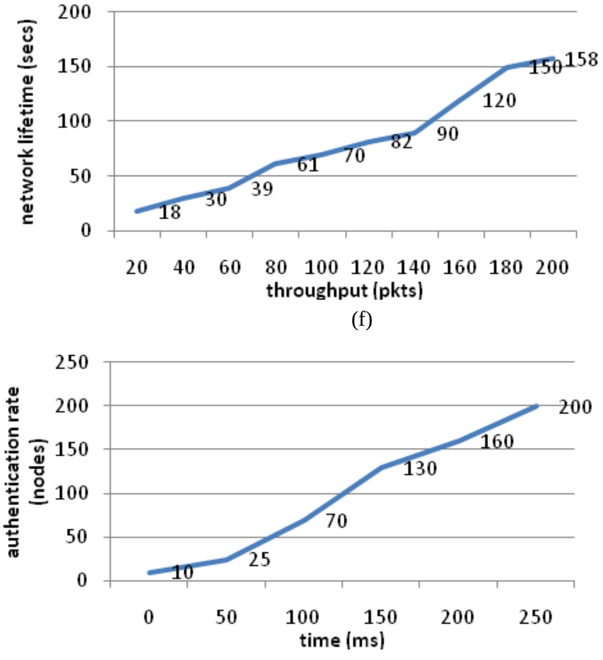
(a)

(b)

(c)

(d)

(e)



(f)

(g)

Figure 2. Performance measure of TSRF

**TRS**

The packet delivery ratio is in decreasing status as shown in Figure 3(a). 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. 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 3(b). Network stability rate also decreases due to straight forward assessment of trust evaluation and it is shown in Figure 3(c). 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 3(d). Thus, the integrity of packets increases. The delay discussed during delivery of packets is shown in Figure 3(e).

Figure 3(f). 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 3(g). 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.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

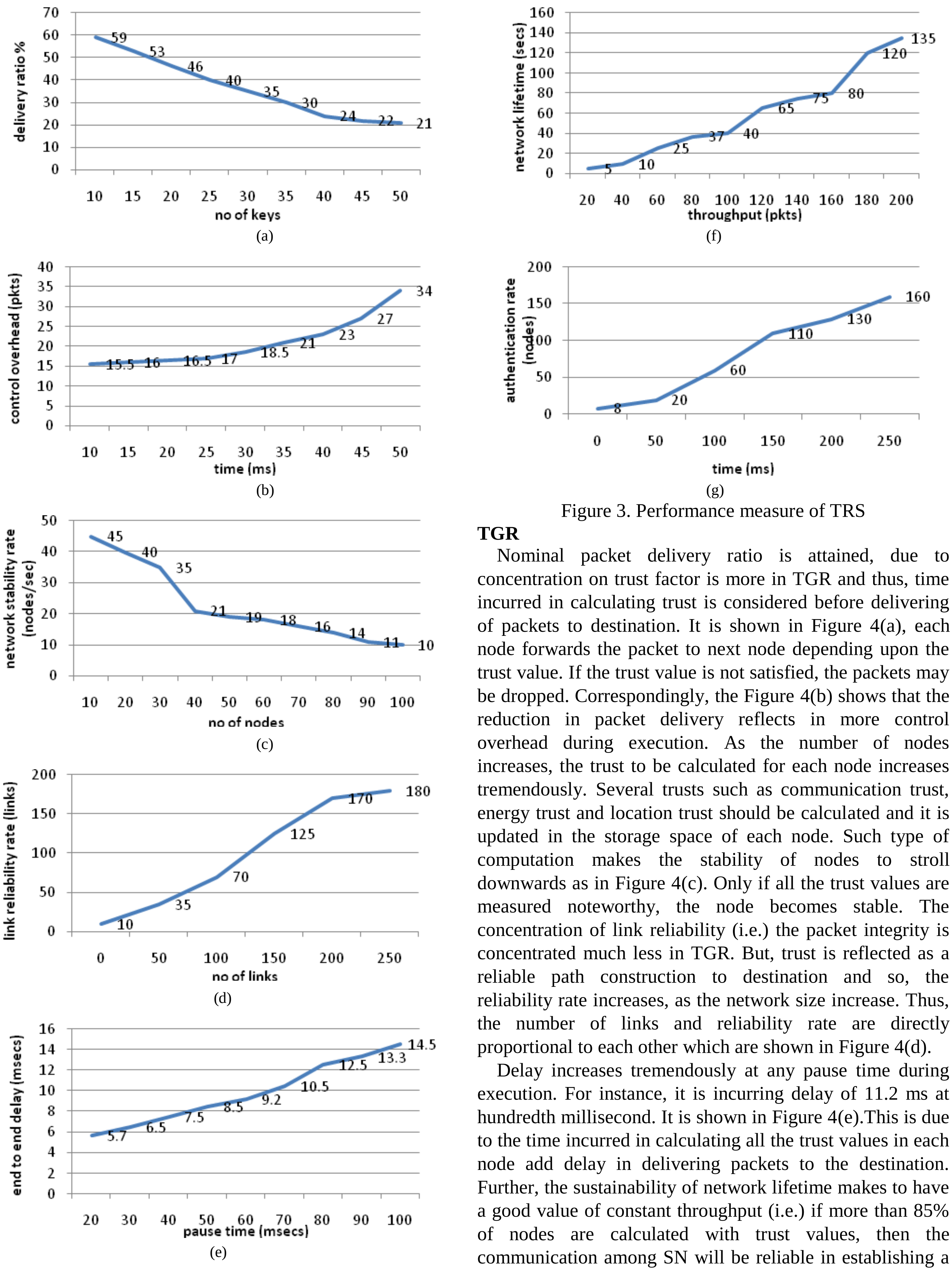
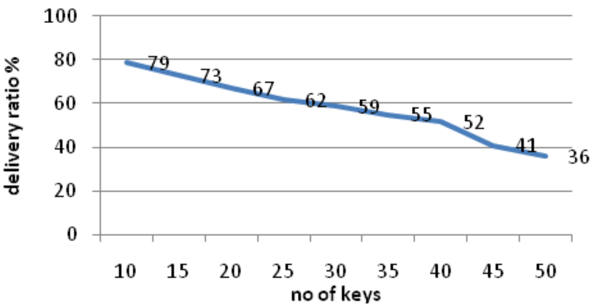


Figure 3. Performance measure of TRS

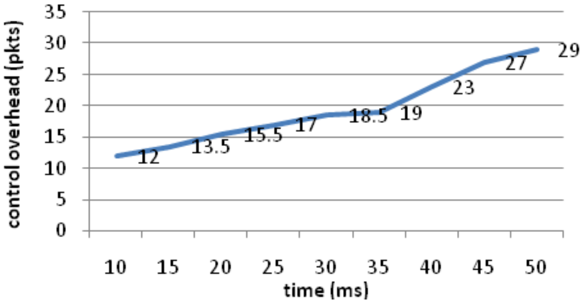
**TGR**

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 4(a), 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 4(b) shows that the reduction in packet delivery reflects in more control overhead during execution. 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 4(c). 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 are shown in Figure 4(d).

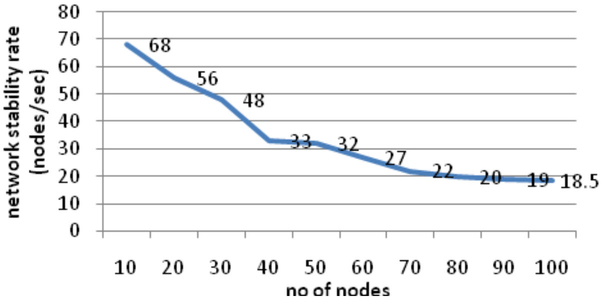
Delay increases tremendously at any pause time during execution. For instance, it is incurring delay of 11.2 ms at hundredth millisecond. It is shown in Figure 4(e).This is due to the time incurred in calculating all the trust values in each node add delay in delivering packets to the destination. Further, 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 4(f). 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 4(g).



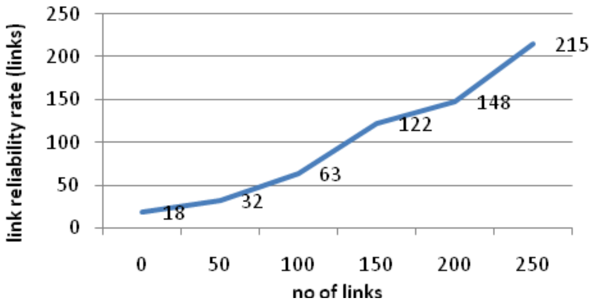
(a)



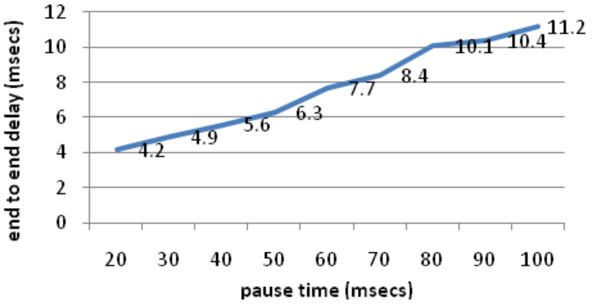
(b)



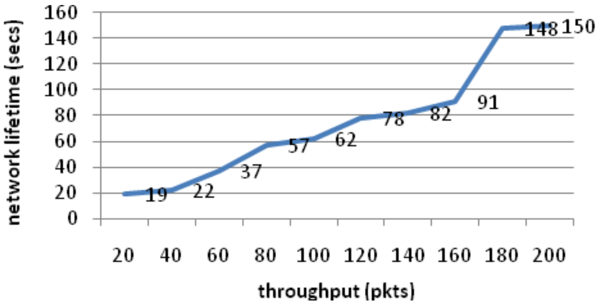
(c)



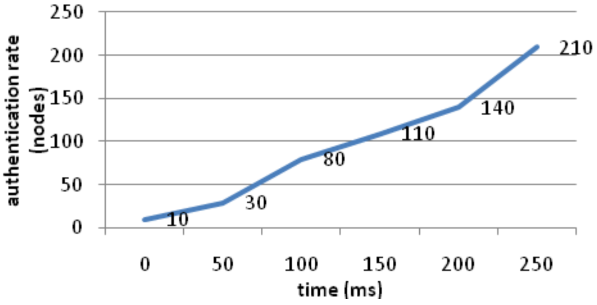
(d)



(e)



(f)

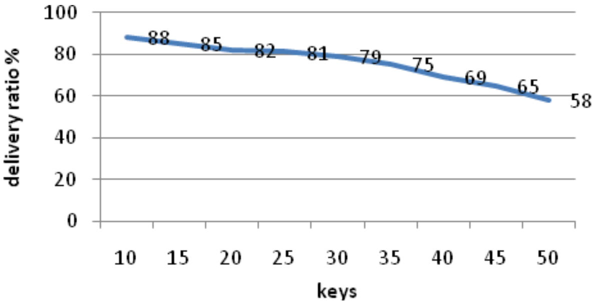


(g)

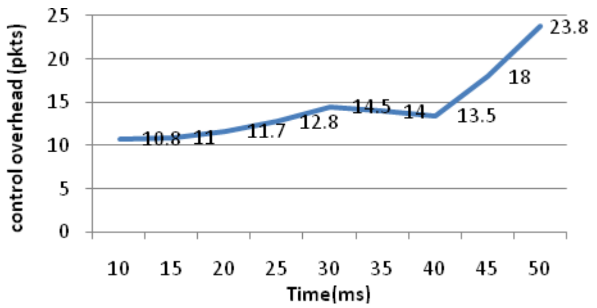
Figure 4. Performance measure of TGR

**PTAP**

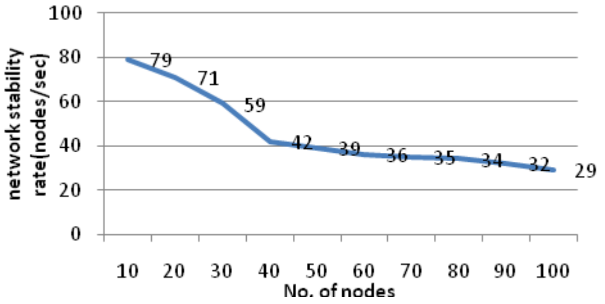
PTAP results in better delivery ratio when compared with other trust authentication protocols in figure 5(a), this is due to implementation of estimation methods to identify legitimate nodes. The delivery of data packets is performed through these legitimate nodes. Minimum overhead is incurred in PTAP as shown in the figure 5(b) is due to less complexity of keys generated through Dual Key Optimization (DKO) methodology in PTAP. The network stability rate that is shown in figure 5(c) is for 100 nodes scenario. Due to trust evaluation methods and secrecy maintained using encryption process made PTAP to deliver data packets and control packets through a stable links. PTAP maintains high reliability rate as shown in figure 5(d) since the link reliability is calculated based on reliability factor of trust evaluation. Due to the channel quality and reliable link selection, it is shown in the figure 5(e) that PTAP achieves less delay when compared to other authentication protocol. When the number of epochs to links increases, the system must rely on high network lifetime as shown in the figure 5(f). Pairwise key generation methodology by DKO is being adopted by PTAP and thus the authentication rate reaches greater heights when compared with other trust authentication protocols. The authentication rate is shown in the figure 5(g).



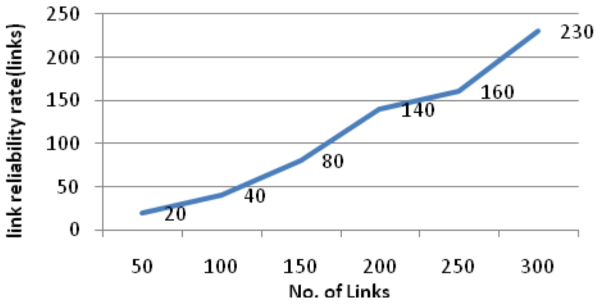
(a)



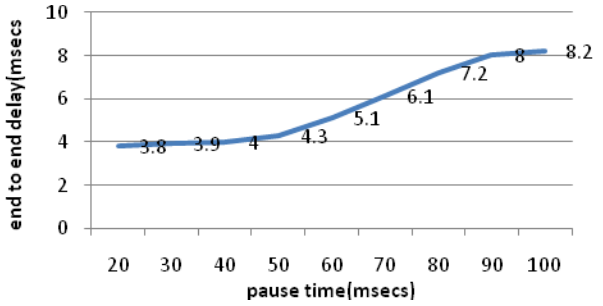
(b)



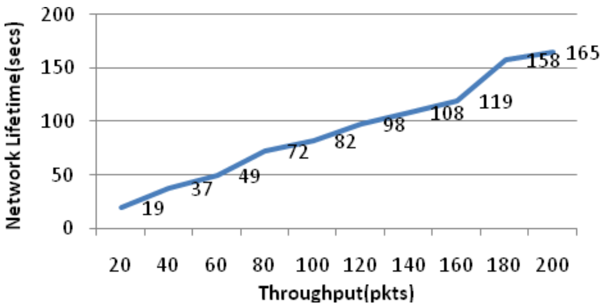
(c)



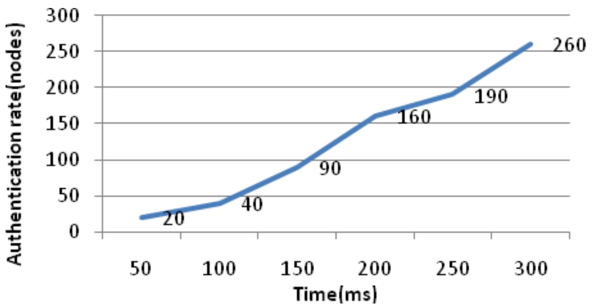
(d)



(e)



(f)



(g)

Figure 5. Performance measure of PTAP

## IV. ATTACK SCENARIOS

### Sybil Attack

Sybil attack occurs due to unauthorized node illegitimately taking multiple identities. The node which captures additional identities is called as Sybil Nodes. Sybil attacks can be performed in various dimensions. The direct communication is making the Sybil node to communicate with legitimate node where the legitimate node send a radio signal which would then heard by sybil node. Indirect communication is one or more malicious nodes claims to reach Sybil nodes. Thus messages are sent to Sybil nodes via malicious nodes. The Sybil node get an identity in two ways, one is fabrication that is, if a legitimate node is identified by 32 bit integer then the attacker can assign each Sybil node by random 32 bit integer. Another way, stolen identities that is if name space is limited, then random integer could not be assigned and thus using a stolen identity.

Detecting Sybil nodes = $\frac{x}{N}$

Probability of not detecting = $\frac{N-x}{N}$

If the test repeated for r rounds then, $\left(\frac{N-x}{N}\right)^r$

Suppose in a set of $N$ neighbors of a node, there are $x$ Sybil nodes, $i$ illegitimate nodes and $l$ legitimate nodes.

***Execution:*** If there are 5% of nodes are created as sybil nodes then the remaining legitimate and illegitimate nodes differ from one protocol to another.

### Black Hole Attack

Black hole attack is exhibited by malicious node through claiming itself as shortest path to destination. The source sends the message through the malicious node after receiving false RREP. The malicious node won't forwards the message or it will discard the packet.

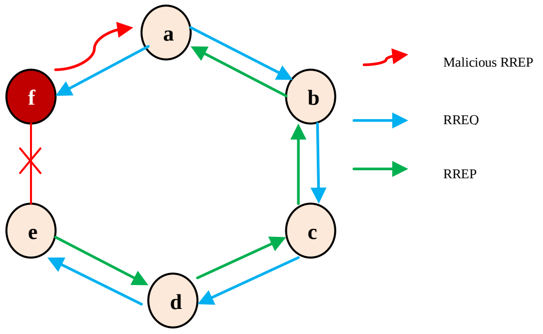


**Figure 6.Nodal diagram showing RREP and RREQ**

The figure 6 states about the single black hole attack in which node $f$ is a malicious node which prohibits the transmission from node $e$. Also, it sends malicious RREP to node $a$ .Further, node $a$ will send all authenticated information through node $f$.

Another type is collaborative black hole attack where some set of nodes collaborate together to malfunction the normal routing process.

***Execution:*** In a 100 node scenario, 5% of nodes are created as fake nodes which will send false RREP. Such false RREP would misdirect every nearest neighbor and multiply throughout the network.

### Tampering

Tampering is similar to compromising of nodes. Physically modifying and damaging the sensor nodes are physical tampering. By performing tampering on a node, the node would extract cryptographic information such as cryptographic key and other confidential data. Tampering make the captured node to be compromised and the compromised node comes under the control of malicious node.

***Execution:*** Five sets of tampering are created in which one malicious node is capturing the cryptographic key information of five nodes. These five nodes are compromised nodes which in turn elaborate to perform further compromising depending upon the trusted authentication protocol.

### Replication Attack

Replication attack is an application dependent attack which exclusively plays a dominant role in WSN. Any adversary can implement such attack by constructing a low cost sensor node to behave as legitimate node. In order to perform this, the adversary has to physically capture the node, reveal the secret credentials, and replicate it in large volume. By doing this, the adversary is able to misdirect the network.

***Execution:*** In the 100 nodes deployment scenario, in order to make a new sensor to be a replicated node, one of the legitimate nodes should be made as dead node. By revealing the secret credentials of legitimate node, the replicated node acts as a malicious node. Initially, one node is replicated and in course of time after receiving authenticated information from other legitimate nodes, more replication can be done. In timestamp $t_1, t_2, t_3, t_4 \text{ and } t_5$ five sensor nodes are replicated.

## V. IMPLEMENTATION OF ATTACK SCENARIO

Implementation begins by creating attack scenario using FakeAgent file which runs the logic of each attack scenario. MyNode file add the percentage of nodes that are going to act as fake nodes corresponding to attack logic. Steps for running fake nodes during execution of trust authentication protocol are as follows.

**Step 1:** Add New Agent
ns-allinone-2.34/ns.2.34/test
folder/FakeAgent.cc

**Step 2:** Edit ns-allinone/ns.2.34/Makefile.in
Add the following line in OBJ_CC section
test/FakeAgent.o \

**Step 3:** Recompile NS-2
Open terminal and go to ns-allinone-2.34/
ns-2.34
directory and type
./conFigure
make
make install

**Step 4:** Run FakeAgent.tcl file

**Step 5:** Adding fake nodes during execution
ns-allinone-2.34/ns.2.34/test
folder/MyNode.cc

**Step 6:** Repeat STEP 2, 3 and 4 for MyNode.cc and corresponding MyNode.tcl file

The simulation settings prescribed in the Table II is executed for all the five trust authentication protocol such as TRS, TARF, TSRF, TGR and PTAP.

TABLE I. SIMULATION SETTINGS AND PARAMETERS

| | |
|---|---|
| No. of Nodes | 100 |
| Area Size | 1300 X 1300m$^2$ |
| Mac | 802.11 |
| Radio Range | 200m |
| Simulation Time | 100 sec |
| Traffic Source | CBR & Poisson |
| Packet Size | 512 bytes |
| Mobility Model | Random Way Point |
| Protocol | AODV |

## VI. RESULTS AND DISCUSSION

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 remaining legitimate nodes are shown in Table II.

The Figure 7 is graphically plotted by referencing Table II.

TABLE II. NUMBER OF LEGITIMATE NODES REMAINING AFTER ATTACK EXECUTION

| Schemes / Attacks | Number of legitimate nodes remaining in 100 nodes scenario | | | | |
|---|---|---|---|---|---|
| | PTAP | TSRF | TGR | TARF | TRS |
| Sybil Attack | 94 | 80 | 90 | 81 | 90 |
| Tampering | 88 | 72 | 75 | 69 | 67 |
| Black Hole | 92 | 93 | 78 | 72 | 74 |
| Identity Replication | 95 | 77 | 92 | 84 | 94 |

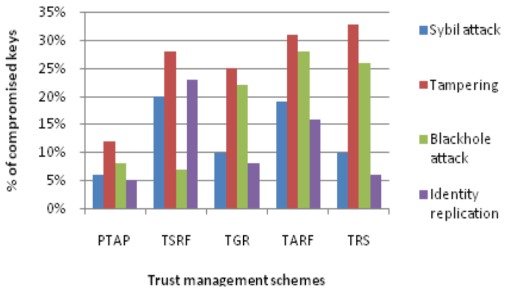


**Figure 7. Survival of attacks in trust management schemes**

## VII. CONCLUSION

The performance of trust authentication protocols such as TARF, TSRF, TRS, RGR and PTAP is analyzed. In order to disseminate the security capability of these protocols, some fake attack scenarios are generated. The number of legitimate nodes remaining in 100 nodes scenario is measured by executing these attack during simulation. The analysis shows that, PTAP outperforms than other trust authentication protocols due to efficient pairwise key generation and security capabilities.

## ACKNOWLEDGMENT

Greatest thanks go to Dr. N. Umamaheswari and Dr. R. Venkatesh for finding and objectifying the research topic. More details of this design are available in our technical report. We must also express our gratitude to the anonymous reviewers for their very helpful comments.

## REFERENCES

[1] William, S, ‘Cryptography and network security principles and practice’, 3rd Edition, Prentice-Hall, 2000.

[2] Tubaishat, M & Madria, S, ‘Sensor networks: An overview’, IEEE Potentials, vol. 22, no. 2, pp. 20-23, 2003.

[3] Chee-Yong, C & Kumar, SP, ‘Sensor networks: Evolution, opportunities, and challenges’, Proceedings of the IEEE, vol. 91, no. 8, pp. 1247-1256, 2003.

[4] Chan, H & Perrig, A, ‘Security and privacy in sensor networks’, IEEE computer journal, vol. 36, pp. 103-105, 2003.

[5] Culler, DE & Hong, W, ‘Wireless sensor networks’,Communication of the ACM, vol. 47, no. 6, pp. 30-33, 2004.

[6] Doru E. Tiliute, ‘Security of Mobile ad-hoc Wireless Networks. A Brief Survey’, Advances in Electrical and Computer Engineering, vol 7(14), number 2(28), 2007.

[7] David, B, Thomas, N, ‘Securing wireless sensor networks: security architectures’, journal of networks, vol. 3, no.1, pp. 65-77, 2008.

[8] Javier, L & Jianying, Z, ‘Overview of wireless sensor network security’, Wireless sensor network security, vol. 1, pp. 1-21, 2008.

[9] Revathi, V, Scott, M, Bhaskar, K & Rama Rao, T, ‘Trust-based backpressure routing in wireless sensor networks”, International journal of sensor networks, vol. 17, no. 1, pp.1-15, 2009.

[10] Theodore, Z, Helen, CL, Panagiotis, T & Stamatis, V, ‘Trust management in wireless sensor networks’, European transactions on telecommunications, pp. 386-395, 2010.

[11] Guoxing Zhan, Weisong Shi & Julia Deng , ‘TARF: A Trust-Aware routing framework for wireless sensor networks’, Springer, pp. 65-80, 2010.

[12] Manjula, V & Chellappan, C, ‘The replication attack in wireless sensor network: analysis and defenses’, Advances in network and communication, vol. 132, pp. 169-178, 2011.

[13] Aveek, C,Vishal, P&Atin, R, ‘A trust based routing scheme for wireless sensor networks’, Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering, springer, vol. 84, pp.159-169, 2012.

[14] Vidya, M & Reshmi, S, ‘Denial of service attacks in wireless sensor network’, International Journal on Advanced Computer Theory and Engineering, vol. 3, no. 2, pp. 16-21, 2014.

[15] Rajaram, S, Babu Karuppiah, A & Vinoth Kumar, K, ‘Secure routing path using trust values for wireless sensor networks’, International Journal on Cryptography and Information Security (IJCIS), vol. 4, no. 2, pp. 27-36, 2014.

[16] Junqi, D, Dong, Y, Haoqing, Z, Sidong, Z & Jing, Z , ‘TSRF: A trust-aware secure routing framework in wireless sensor networks’, International Journal of Distributed Sensor Networks, vol.2014, pp. 1-15, 2014.

[17] Geetha, V & Chandrasekaran, K, ‘A distributed trust based secure communication framework for wireless sensor network’, Wireless sensor network, scientific research, vol. 6, no. 9, pp.173-183, 2014.

[18] Joby, PP & Sengottuvelan, P, ‘A survey on threats and security schemes in wireless sensor networks’, International journal of engineering research and applications, vol. 5, no. 1, pp. 89-94, 2015.

[19] Raghini, M, Umamaheswari, N & Venkatesh, R, ‘PTAP: Pair key based trust authentication protocol for authentication in WSN’, Journal of computational and theoretical nanoscience, vol. 13, no. 3, pp. 1701-1708, 2016.

[20] Raghini, M, Umamaheswari, N & Venkatesh, R, ‘Key establishment in wireless sensor network using dual key optimization (DKO)’, Journal of convergence information technology, vol. 11, no. 3, pp. 103-114, 2016.

[21] Fenye, B, Ing-Ray, C, MoonJeong, C & Jin-Hee, C 2012, „Hierarchical trust management for wireless sensor networks and its applications to trust- based routing and intrusion detection‟, IEEE transactions on network and service management, vol. 9, no. 2, pp. 169-183.

[22] Theodore, Z, Helen, CL, Panagiotis, T & Stamatis, V 2010, „Trust management in wireless sensor networks‟, European transactions on telecommunications,pp.386-395.

## AUTHORS PROFILE

**Dr. M.Raghini** completed B.Tech Information Technology & M.E. Computer Science and Engineering degree in P.S.N.A College of Engineering, Dindigul under Anna University, Chennia, in 2006 and 2008 respectively. She completed her Ph.D in the Faculty of Information and Communication Engineering, under Anna University Chennai, in 2017. Currently she is working as Associate Professor in Department of CSE, K.L.N. College of Engineering, Madurai. She has published more the 30 papers in international conferences and journals. She is also a reviewer for two International Journals. She has received Research Excellence Award from IEAE, Best research practices in the department from ICT academy and outstanding contribution award from management of K.L.N. College of Engineering. Her research interests are Wireless Network, Cyptography and Network Security and Big Data Anlaytics.

**Dr.S. Miruna Joe Amali** completed her B.E. (Computer Science and Engineering) degree in P.S.N.A College of Engineering, Dindigul, under Madurai Kamaraj University, Madurai, in 2001 and the M.E. (Computer Science and Engineering) degree in Thiagarajar College of Engineering, Madurai, under Anna University, in 2005. She completed her Ph.D. full-time research in the Faculty of Information and Communication Engineering, under Anna University, Chennai. She also has industry experience and has worked in HCL Technologies, Chennai as Lead Engineer. Currently she is working as Professor in Department of CSE, K.L.N. College of Engineering, Madurai. She has published 24 journal papers and has an h-index of 7 and i10-index of 4. She is also a reviewer for four International Journals. She has received Research Excellence Award from IEAE, Best research practices in the department from ICT academy and outstanding contribution award from management of K.L.N. College of Engineering. She has also filed for an Indian patent along with two faculty members. She has authored two text books and one technical chapter under Scopus publication. Her research interests are Soft Computing, Evolutionary algorithms specifically Differential Evolution, surrogate model integration and their applications to Engineering Optimization problems.

**Brindha Subburaj** completed her bachelors and masters degree in computer science and Engineering in the year 2010 and 2012 respectively from Anna University. Currently she is pursuing research in the field Engineering Optimization. Her research interest includes networking, machine learning and cloud computing. She has 7 years of academic experience and published research articles in several international conferences and journals.