Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 4): pp. 6638-6657
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.04.765068

Trust Based Localization Technique

T.P.Rani , J.Aruna Jasmine , S.Susila Sakthy

Sri Sairam Engineering College Chennai

Abstrat

The applications of wireless sensor network (WSN) ranges from Area monitoring, Healthcare monitoring and Environmental sensing to the impervious applications like structural health monitoring and ocean monitoring systems. Due to this proliferated use and open nature of WSN, security issues have become a prime concern. Most of the attacks aim on energy deprivation, as energy is one of the major resource constraints in WSN. Trust based systems enhance network security. By incorporating Trust with Localization, our proposed system aims to thwart various types of attacks including replicated node attack which focuses on energy destitution. It is observed that the existing methods Light weight detection systems and the Trust aware systems incur lesser probability of detection rates in comparison with the proposed Trust based Localization Technique (TBLT). TBLT is a distributed technique but incurs overhead. But it can be considered as a tradeoff against the predication rate and throughput. The simulations are performed in NS2 and results are analyzed.

1. Introduction

Security in Wireless sensor network (WSN) is gaining the momentum in today's era asWSN finds its prominence in all domains and due to the openness of the nodes [1-2]. A sensor network comprises of elements which have capability to sense, compute and forward information such that the administrator or the base station can manage the scenario [3-5]. The WSN provides theservices such as monitoring, alerting, providing information on demand and actuating [3], and it is the main focus in Internet of things (IOT) [6]. Due to its proliferation and inevitable use, the security issues have taken its turn as the sensor nodes are generally not incorporated with the security shields due to cost concerns. But all applications do not demand the security concern in WSN. The application of a WSN ranges from Air conditioners (AC) for household to Smart homes and cities [7]. WSN is widely used in reconnaissance applications. Such military applications demand security shields [7]. As in any networks, availability, repudiation, authentication, data freshness and robustness are the security requirements in WSN [8-9].

Security may be achieved by cryptographic measures like key management or secure routing. But when a node is compromised, the key may be obtained. Hence key management alone is not sufficient [10-11]. Hence we have used Trust mechanisms along with Key management. The system serves as an Intrusion Detection System (IDS) [12] and is tested against selfish node attacks, flooding attacks and replicated node attacks. Localization techniques are used by which a node estimates its location and using this mechanism replication attack is overcome. The system providessecurity to the WSN by incorporating Key management, Trust and Localization techniques. WSN nodes are resource constrained. Optimizing energy is a must in implementing any algorithm in WSN [13]. The energy optimization is justified by analyzing the performance of the network and the system is compared with existing system. The rest of the paper is organized as follows. In section II the related works of Trust management systems existing in WSN are portrayed. In SectionIII, the implementation of the proposed technique is dealt. The Performance analysis is furnished in Section IV, followed by Conclusion in V.

2. Related Works

Trust is a value based on past behavior of entities [13]. Trust is subjective and may be based on many functional parameters such as authenticity of data, connectivity of the path, processingcapability of a node and availability [14]. Trust can be calculated based on policies or reputation [15]. The characteristics of trust are subjective, transitive, reflexive and context-sensitive [14]. In addition to general security trust is applied in access control, aggregation, routing, monitoring and IDS [13].A literature survey on trust in other domain such as Peer to Peer Networks (P2P), Mobile Adhoc Networks (MANET), social networks, internet applications and cognitive radio is available in [16 -20].

In LDTS [21], the trust calculation and evaluation is done for Hierarchical networks. The interactions between cluster members (CM) to cluster heads (CH) and cluster heads to Base station is considered for trust computations and evaluation. But the method can be applicable only on hierarchical networks.

In TAWSN, the trust is used for evaluating the nodes behavior in clustered systems [22]. The method focuses on clustered systems and it cannot overcome replication attacks as localization techniques are not applied.

Self-localization has become an inevitable feature required in WSN. In applications like environment monitoring systems, forest fire or military surveillance systems, data without source is illogical. [23]. Integrating GPS into all nodes of WSN for the purpose of localization poses the problem of price hike. Hence localization techniques with minimal overhead are opening research interest in WSN. A survey on distributed and centralized localization techniques is portrayed in [23-24].

3. Proposed System

In the sensor networks, the nodes are deployed in the random manner where each node is provided with the unique node id through which the nodes broadcast the message acrossthe network. The nodes are assigned its private and public key during deployment. Using neighbor public key and its own private key nodes generate common key for neighbor communication. The node key generation is done using elliptic curve digital signature algorithm (ECDSA) [25]. Figure 3.2.1 explains the algorithm of the proposed system and table 3.2.1 explains the terms that are used in the algorithms and in the further explanations. In the following sections each phase implemented is explained.

Algorithm- TBLT working method

```
while(1)
{
// Phase I
If BS ready then
    Broadcast the key share (k) message
If node i receives k messages then
    Create the neighbor table (k, ID)
If node receives data packet then
    If ( $k_1$==$k_2$)
    Compute direct trust $T_D$fori$_n$
If node j∉neighborset then
If j send recommendation of i then
    Compute indirect trust $T_I$ for i$_j$
    Compute $T=T_D + T_I$
If T < 0.5 then
Set malicious node
Update neighbor table (T, ID)
//Phase II
Obtain the RSSI$_1$, RSSI$_2$, RSSI$_3$values and d1, d2 & d3 of three nodes N1,N2 and
N3 with respect to the node Nu whose coordinates xu and yu needs to be
computed.
From the above values compute the x and y coordinates (x1,y1), (x2,y2) and (x3,y3)
For the unknown node compute Location (xu,yu) as Li from the above
obtainedvalues
If (id[i] is available in $L_1$&$L_2$)
If(L1~L2 >TH)
    Revoke id
Update neighbor table
}
```

Figure 3.2.1

S.no	Terms	Use
1.	K	Shared Key

2.	ID	Node identifier
3.	T_D	Direct trust value
4.	T_I	Indirect Trust value
5.	T	Total Trust (T_D + T_I)
6.	RSSI	Received Signal Strength Indicator
7.	D	Distance between the nodes
8.	L	Location of the node (x,y)
9.	Id	Local node identifier

Table3.2.1

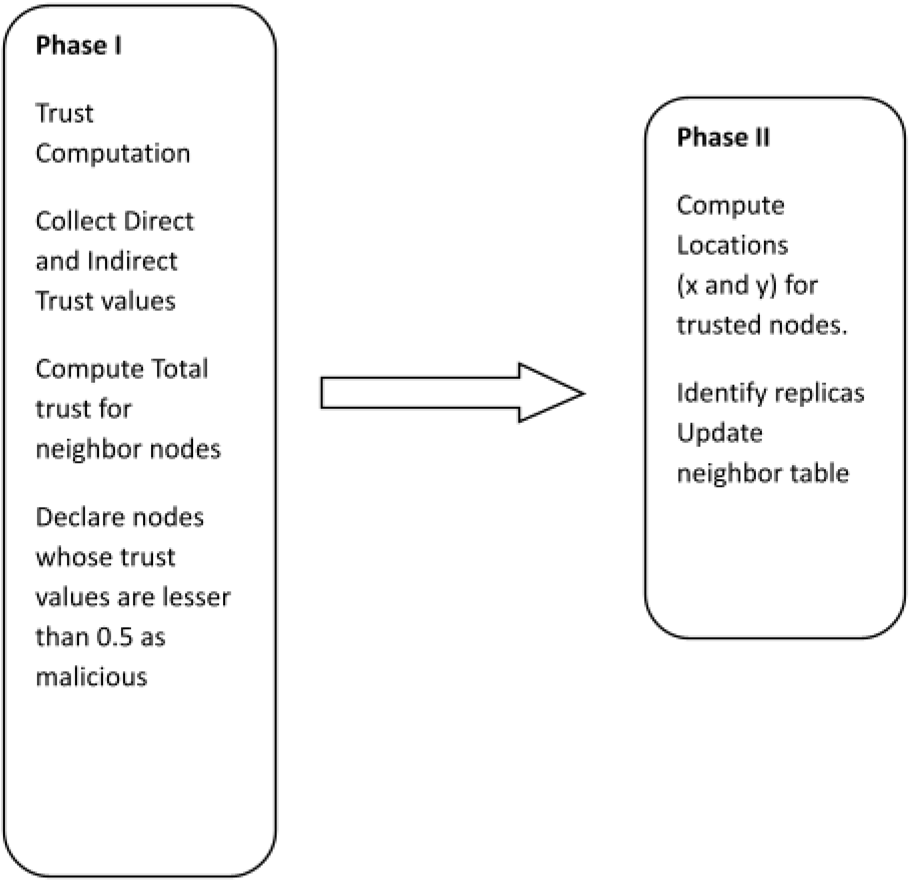

Phase I
Trust Computation
Collect Direct and Indirect Trust values
Compute Total trust for neighbor nodes
Declare nodes whose trust values are lesser than 0.5 as malicious
Phase II
Compute Locations (x and y) for trusted nodes.
Identify replicas
Update neighbor table

Figure 3.3.2 Phases of TBLT

Phase I - Trust Computation

In phase I the nodes compute direct and indirect trust values [13]. Based on these computed trust values, nodes are termed as trusted and distrusted nodes.

Direct trust computation

Once the event of message broadcasting takes place, the trust computation for each of the node is started. The direct trust is computed based on direct observations of each node that participates in data transfer. When the nodes starts communicating it exchange a key share message between the nodes, if both neighboring nodes has common key it will rebroadcast the message to destination. The direct trust is computed with the parameters like Message Authentication Code (MAC), cipher text, correctness of the node and selfishness of the node.

Direct trust: This is computed between the direct observations based on the parameter

1. tmac(i) message authentication for node i, this checks whether the received packet is modified or not. When MAC matches it is taken as 1 otherwise 0.
2. tct(i) checks the cipher text is decrypted into meaningful or not where it is taken as 1 when it is true or 0 when it is false.
3. tc(i) correctness of node is based on the behavior of the node which returns the status of the nodeand the value is taken from 0 to 1.
4. tfi(i) selfishness of node is calculated by, tfi(i) = no. of packets actually forwarded/ no of packets supposed to be forwarded

For each of these parameters weight value is assigned based on the priority of the parameters and hence the direct trust is calculated by

$$TD= tmac(i) *w1 + tct(i) *w2 +tc(i) *w3 + tfi(i)*w4$$

Indirect trust computation

The indirect trust is obtained from recommendations of other nodes that are not in the vicinity region but had a previous interaction with the node. The indirect trust is computed with theparameters of data forwarding, unwanted flooding and behavior monitoring

The indirect trust is computed based on the recommendation of the nodes.

1. $t_{df(i)}$ data forwarding specifies the number of packets transmitted from the Source iscomputed by

$t_{df(i)}$ = no.of.packets forwarded/ no.of.packets expected

2. $t_{uf(i)}$ unwanted flooding specifies the unwanted flooding or dropping of packets at the sink and it is computed by $t_{uf(i)}$ = no.of.packets sent/time
3. $t_{bm(i)}$behavior monitoring specifies the behavior of the node for a packet
4. either it forwards or send to wait state, it is

given by$t_{bm(i)}$ = (no.ofpackets sent/time)

$T_I= (\sum t)/m$ (1)

Where

tm= tdf(i) * w1 + tuf(i) *w2 + tbm(i) *w3 (2)

$\sum t = t_{m1} + t_{m2} + ... + t_{mn}$ (3)

m= number of neighboring verifier nodes

The overall trust is computed from direct as well as indirect trust calculation $T=T_D+T_I$(4)

T_D- total direct trust T_I- total indirect trust Where $\sum w =1$

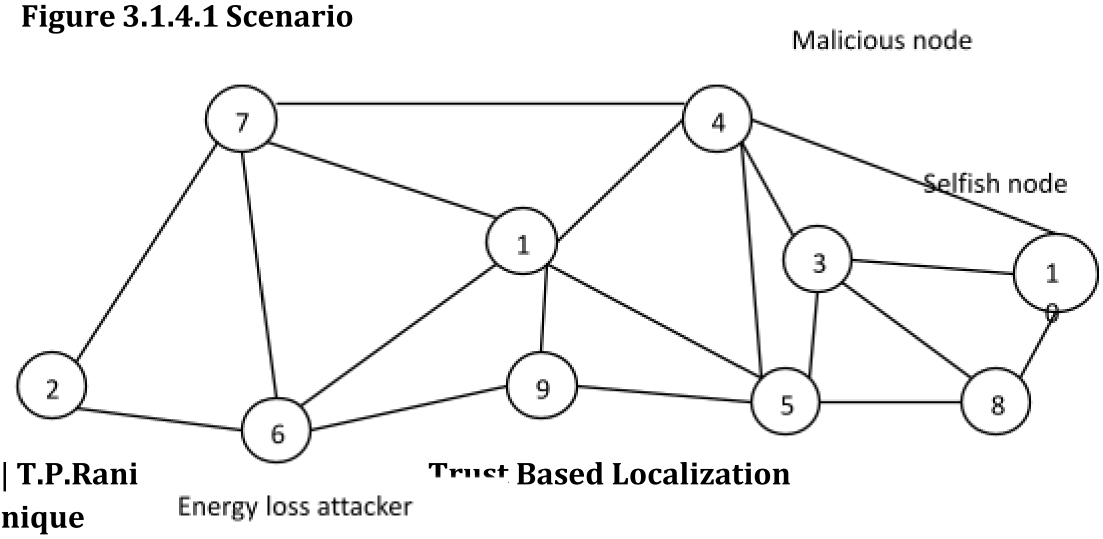
When the T is less than 0.5 then the nodes are identified as untrusted nodes and such nodesare eliminated.

Detection of malicious node

The malicious node is detected based on the opinion generated by the trust evaluation process. When the trust value evaluated from the direct and indirect method is less than 0.5 then the node is termed to be malicious or distrusted node, considering at least fifty percentof the node is genuine. Using the trust computation attacks such as selfish node attack, and flooding attackcan be identified and these nodes can be removed from neighbor table and thereby further communication between the malicious nodes is not entertained. A scenario for trust computation is created as shown in Figure3.1.4.1 and results are evaluated. The nodes 6, 4 and 10 are malicious nodes in the scenario. The neighbor tables and the weights assumed for parameters are given in Table 3.1.4.1. The Trust values calculated as per the scenario and corresponding neighbor table updates are given in tables 3.1.4.2.

Trust Computation Scenario

Figure 3.1.4.1 Scenario



NEIGHBOUR TABLE		WEIGHT VALUES	
Node	Neighbors	**Parameters**	**Weights**
2	6,7	tmac(i)	0.1
7	2,6,1,4	tct(i)	0.1
6	2,7,1,9	tc(i)	0.2
1	7,6,9,4,5	tfi(i)	0.2
9	1, 6, 5	tdf(i)	0.1
5	9, 3, 1,4,8	tuf(i)	0.2
4	5, 3, 1,10	tbm(i)	0.1
10	4, 3, 8	TD	0.6
8	5, 3, 10	T_I	0.4

Table 3.1.4.1

Node	Tmac	Tct	Tc	Tfi	Tdf	Tuf	Tbm	td	ti	T
6	1	1	0	1	0	0	0	0.4	0	0.4
7	1	1	1	1	1	1	1	0.6	0.4	1

Node	Neighbor	Trust
2	7	1

Node	Tmac	Tct	Tc	Tfi	Tdf	Tuf	Tbm	td	ti	T
1	1	1	1	1	1	1	1	0.6	0.4	1
2	1	1	1	1	0	1	1	0.6	0.3	0.9
4	0	0	0	0	0	1	0	0	0.2	0.2

Node	Neighbor	Trust
7	1	1
	2	0.9
	4	0.2

Node	Tmac	Tct	Tc	Tfi	Tdf	Tuf	Tbm	td	ti	T
7	1	1	1	1	1	1	1	0.6	0.4	1
9	1	1	1	1	1	0	1	0.6	0.2	0.8
5	1	1	1	1	1	1	1	0.6	0.4	1

Table 3.1.4.1

Node	Neighbor	Trust
1	7	1
	9	0.8
	5	1

Node	Tmac	Tct	Tc	Tfi	Tdf	Tuf	Tbm	td	ti	T
1	1	1	1	1	1	1	1	0.6	0.4	1
9	1	1	1	1	1	0	1	0.6	0.2	0.8
3	1	1	1	1	1	1	1	0.6	0.4	1
8	1	1	1	1	1	1	1	0.6	0.4	1

Trust value for neighbors of node 2:

Node 6 is eliminated from the neighbor table

Trust value for neighbors of node 7:

Node 4 is termed as malicious node and eliminated, the updated neighbor table.

Trust value for neighbors of node 1:

Node 6, 4 is eliminated from the neighbor table

Trust value for neighbors of node 5:

Node 4 is eliminated from the neighbor table

The updated neighbor table of node 5 is

Node	Neighbor	Trust

5	1	1
	9	0.8
	3	1
	8	1
Trust value for node 10: Node 10 is termed as selfish node.		

Node	Tmac	Tct	Tc	Tfi	Tdf	Tuf	Tbm	td	ti	T
1	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0.2**	**0.2**	**0.4**

Table 3.1.4.2

Phase II – Localization Computation

The resultant Network obtained from Phase I,with updated neighbor tables will be free from nodes involved in malicious activities such as flooding and selfishness. But there may be nodes which may be replicated and still do not show any sign of maliciousness as they areinvolved only in monitoring the scenarios. At present they cannot be identified as they are not involved in malicious activity. It can be resolved in Phase II. Applying Localization technique, the locality of all trusted nodes are calculated, and if a node is found to have two locations, then it is compared with a nominal threshold TH. A node with a speed s can beable to travel to a distance within the threshold TH. If the nodes locations vary then the nodes is declared as replicated and the neighbor tables are updated. The steps involved in Phase II are presented in the following section.

In this phase the locality of trusted nodes are computed. The proposed system uses triangulation method and combines Received signal strength indicator (RSSI) and distance between nodes to find the position of the unknown node [26]. This method is propagated among trust worthy nodes, until all trustworthy nodes positions are known.

Applying localization method is required for the network to detect replicationattacks. Replicated nodes attacks detection is done only to the trustworthy nodes so as to provide a two level security. The nodes with their positions reports to the base station and the nodes with dissimilar positions and same id is identified as a replicated node and the replicated node is revoked from further communications.

Localization is done with the triangulation method. It is an example of range based movement which uses the geometric properties of the triangle, where three anchor node is necessary to find the position of the unknown node. The anchor node periodically sendsthe signal where distance from the anchor to the mobile nodes is computed based on RSSI. The RSSI is converted into distance by

RSSI = $P_tG_tG_r\lambda^2$(5)

$(4\pi)^2d^2L$

Where, d is distance
P_t is transmission powerG_tG_r is gain
λ is wavelength

L is loss
Taking the Euclidean distance from the anchor to the node, where the intersection ofthe distance of all the three anchor nodes gives the most accurate position of the node

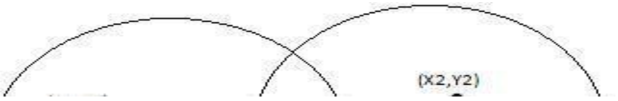


Figure 3.2.1.1 Triangulation
Triangulation Algorithm

1. Process initialization
2. A node (i) calculate L
3. The anchor nodes with coordinates $[X_a,Y_a]$ are known
4. Get RSSI values from $[n_1,n_2,\ldots,n_n]$ for N(i)
5. Strongest RSSI are found and circles are mapped
6. From step(5) 3 values are taken for computation of L
7. Using the Euclidean distance formula the L[N(i)] is doneDistance $[(x_u, y_u)(x_1,y_1)]=\sqrt{(}\ x_u -x_1)\ ^2+(y_u-y_1)^2 =$ d_1 Distance $[(x_u, y_u)(x_2,y_2)]=\sqrt{(}\ x_u -x_2)\ ^2+(\ y_u -y_2)^2 = d_2$ Distance $[(x_u, y_u)(x_1,y_1)]=\sqrt{(}\ x_u -x_3)\ ^2+(\ y_u -y_3)^2 = d_3$
8. End process

With triangulation node with same id is present at two different position areidentified as replication.

Localization Scenario

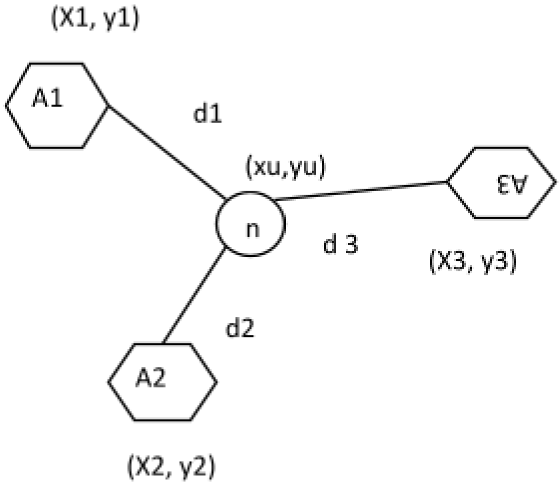


Figure 3.2.2.1 RSSI from A_1= 9.865e^{-09} d^2 = (0.2818)(1.0)(1.0)(1)^2

4(3.14)(1)(9.865e^{-09})

d^2 = 1.4686

d = 1.21185

Similarly the RSSI value from three anchor nodes to a unknown node and their corresponding distance is given below

Anchor Nodes	RSSI	Distance
A1	9.865e^{-09}	1.21185
A_2	3.668e^{-10}	3.2752
A_3	6.784e^{-10}	5.8031

Table 3.2.2.1 Finding the Euclidean distance from anchor to node gives the position of the unknown node.

	X-Coordinate	Y-Coordinate
(x_1,y_1)	109.8	504.8
(x_2,y_2)	301.9	483.3
(x_3,y_3)	265.3	323.6

Table 3.2.2.2

The distance formula is,

Distance $[(x_u,y_u)(x_1,y_1)]=\sqrt{}(x_u-x_1)^2+(y_u-y_1)^2 = d_1$

Distance $[(x_u,y_u)(x_2,y_2)]=\sqrt{}(x_u-x_2)^2+(y_u-y_2)^2 = d_2$

Distance $[(x_u, y_u)(x_1,y_1)]=\sqrt{}(x_u-x_3)^2+(y_u-y_3)^2 =$ d_3Resolving the equation in the matrix form,

$2 \quad (x_3-x_1)\ (y_3-y_1) x_u \quad = \quad (d_1^2-d_3^2) - (x_1^2-x_3^2) - (y_1^2-y_3^2)$

$(x_3-x_2)(y_3-y_2) \quad y_u \quad (d_2^2-d_3^2) - (x_2^2-x_3^2) - (y_2^2-y_3^2)$

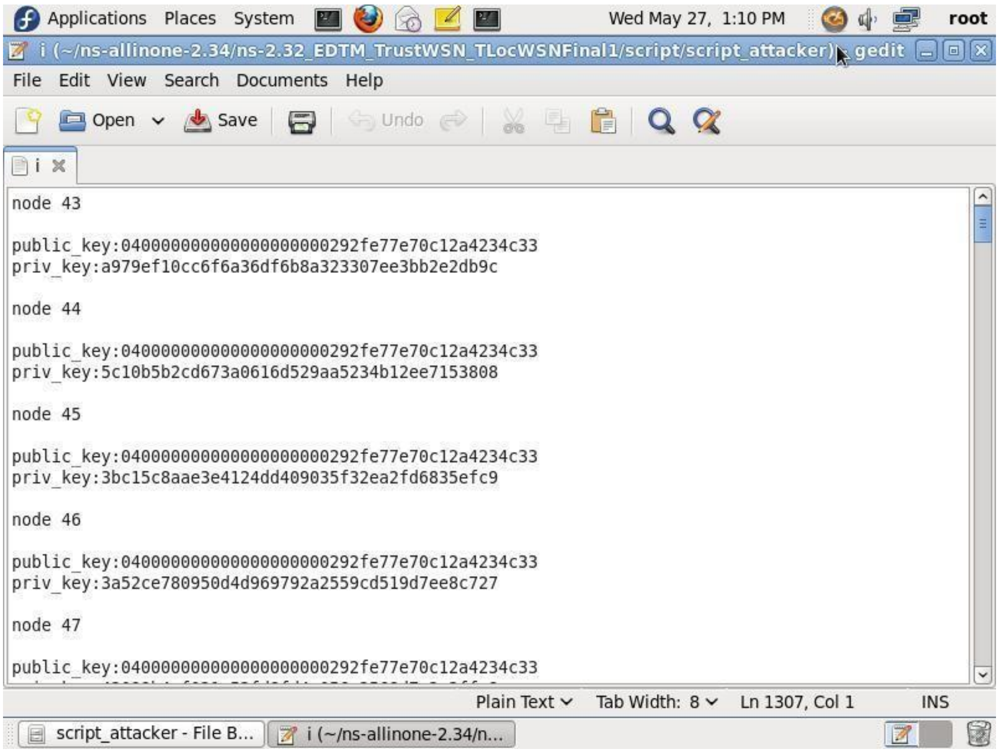
Substituting the values in the above equation gives,311x - 360.8y = -91003.2 — (1)
-73.2 – 319.4y = -149644.37 — (2)

Solving the linear equations (1) & (2) will give the position of $(x_u,y_u)x_u = 198.2$
$y_u = 423.0$

Solving the linear equations (1) & (2) will give the position of $(x_u,y_u)x_u = 198.2y_u = 423.0$

4. Performance evaluation

The system is implemented in NS2 simulator in which nodes are deployed using random way point model. The figure depicts the key share between the nodes.


Applications Places System
Wed May 27, 1:10 PM
root
i (~/ns-allinone-2.34/ns-2.32_EDTM_TrustWSN_TLocWSNFinal1/script/script_attacker) - gedit
File Edit View Search Documents Help
Open
Save
Undo
i
Plain Text
Tab Width: 8
Ln 1307, Col 1
INS
script_attacker - File B...
i (~/ns-allinone-2.34/n...

```
node 43

public_key:040000000000000000000292fe77e70c12a4234c33
priv_key:a979ef10cc6f6a36df6b8a323307ee3bb2e2db9c

node 44

public_key:040000000000000000000292fe77e70c12a4234c33
priv_key:5c10b5b2cd673a0616d529aa5234b12ee7153808

node 45

public_key:040000000000000000000292fe77e70c12a4234c33
priv_key:3bc15c8aae3e4124dd409035f32ea2fd6835efc9

node 46

public_key:040000000000000000000292fe77e70c12a4234c33
priv_key:3a52ce780950d4d969792a2559cd519d7ee8c727

node 47

public_key:040000000000000000000292fe77e70c12a4234c33
```

Figure 9.2 Key share message using ECDSA

No. of malicious nodes	LDTS	TBLT	TAWSN
2	2	2	1
4	3	4	2
6	5	5	3
8	7	8	4
10	8	10	5

Table 9.2 Attacker Vs Detection

The scenario is taken for 90 nodes by varying the attackers and finding out the number of nodes identified from it. The comparison is done with the existing work. The number of detected malicious nodes is proportionate to the number of malicious nodes. The attacker nodes are considered to be flooding nodes as an example.

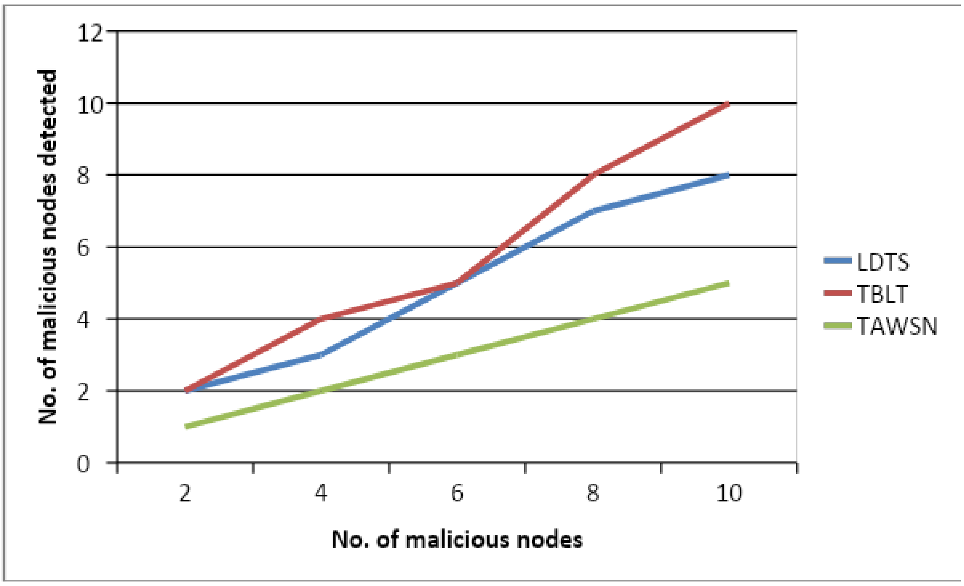
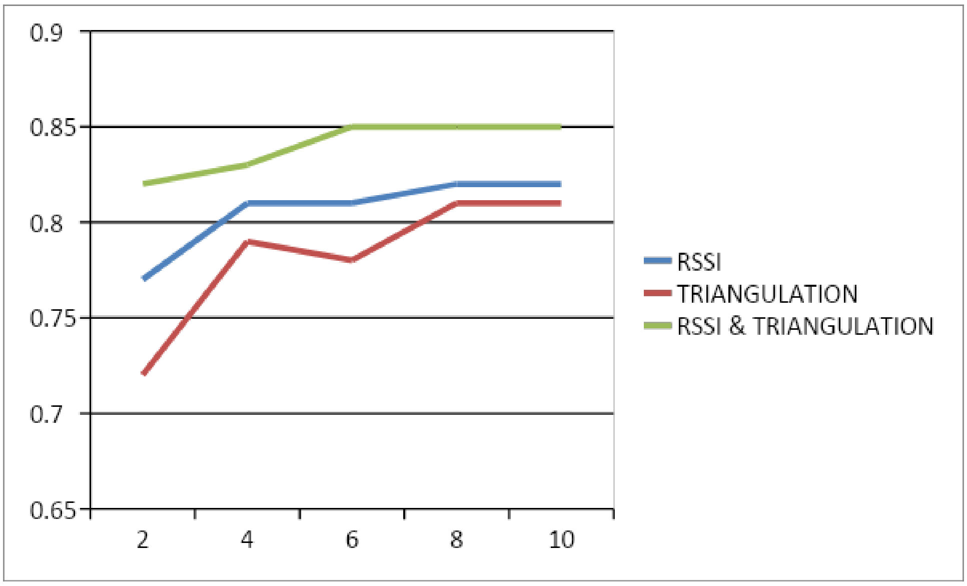


Figure 9.8 Attacker Vs Detection

No. Replica	RSSI	TRIANGULATION	RSSI & TRIANGULATION
2	0.77	0.72	0.82
4	0.81	0.79	0.83
6	0.81	0.78	0.85
8	0.82	0.81	0.85
10	0.82	0.81	0.85

Table 9.5 Attackers Vs Detection rate

The detection rate is calculated by the nodes detected with time interval. The scenario is done by varying the number of replica attacker and the detection rates are obtained. The replica node detection using RSSI, triangulation and TBLT technique, which combines both RSSI and triangulation is analyzed. It is observed that the proposed method is variesin prediction rate from the existing Triangulation method by 4% and RSSI by 3%.



NO. OF MALICIOUSNODES	CONTROL OVERHEAD			THROUGHPUT		
	LDTS	TBLT	**TAWSN**	**LDTS**	**TBLT**	**TAWSN**
2	17.465	20.520	19.2	18.865	27.569	26.7
4	17.780	17.374	17.1	12.406	37.809	30.5
6	18.058	19.187	18.7	11.736	30.641	28.7
8	16.512	19.509	18.8	15.990	29.144	29.2
10	16.269	18.932	18.5	12.209	36.470	32.3

Table 9.3 No. of malicious nodes Vs Control overhead and Throughput

NO. OF NODES	CONTROLOVERHEAD			THROUGHPUT		
	LDTS	TBLT	**TAWSN**	**LDTS**	**TBLT**	**TAWSN**
50	11.433	9.871	9.412	53.484	60.337	61.12

60	12.715	13.592	13.512	19.337	53.287	55.231
70	19.108	15.512	14.513	44.465	43.913	46.512
80	15.307	17.798	16.872	13.193	41.629	42.237
90	16.922	16.696	16.522	15.202	31.625	32.239

Table 9.4 Nodes Vs Control overhead & Throughput

Throughput is the rate of successful message delivery and overhead affects the system complexity.The scenario is done with varying the attackers and the number of nodes and the comparison results with number of nodes shows that our proposed system has 3% of reduced overhead and 77% of increased throughput and with the number of attacker proposed system has 10% of increased overhead and 45% of increased throughput. This increase in overhead is justified withthe security and considered to be a tradeoff for node security.

5. Conclusion

Trust based localization technique (TBLT) combines trust based malicious node detection and localization technique to thwart malicious node attacks and silent replicated node attack. It serves as IDS to detect the presence of these attacks with better prediction rates and throughput when compared to existing techniques. The system incurs overhead but it can be considered as a trade off against the prediction rate. The simulations were performed in NS2 and results obtained are tabulated. The mechanisms to study about the reducing the overhead incurred may be carried out as our future work.

6. References

[1] Renyong Wu, Changsha, Xue Deng, Rongxing Lu, XueminShen, "Trust-based anomaly detection in wireless sensor networks", In Proc. IEEE International Conference on Communications in China (ICCC), 2012, 15-17 Aug, 2012, pp. 203 – 207.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor networks survey", International Journal of Computer and Telecommunications Networking, vol.52, no.12, pp. 2292-2330, August,2008.

[3] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez Gago, "Trust management systems for Wireless sensor networks, Best practices", Computer Communications, vol.33,no.1, pp.1086-1093, 2010.

[4] T.Roosta, A.Shah, B.Sinopoli, A.Giani, G.Karsai, J.Wiley, "A test bed for secure and robust SCADA systems", ACM SIGBED Review, vol.5, no.2, pp.1-4, 2008.

[5] Kazem Sohraby, Daniel Minoli, Taieb Znati, "Wireless Sensor Networks: Technology, Protocols and Applications", April 2007.

[6] Fagen Li, Pan Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things", IEEE Sensors Journal, vol. 13, no. 10, pp. 3677

-3684, June 2013.

[7] I.Y.Akyildiz, W.Su, Y.Sankara Subramaniam, E.Cayirci, "Wireless sensor networks: Asurvey", Computer Networks vol.38, pp. 393-422, 2002.

[8] A.Boukerch, L.Xu and K.EL-Khatib, "Trust based security for wireless ad hoc and sensornetworks", Computer Communications, no.30, pp 2413-2427, 2007.

[9] L.Kagal,T.Finin and A.Joshi, "Trust based security in pervasive computing environments",IEEE Computer, vol.34,pp. 154-157, 2001.

[10] Guangjie Han, Jinfang Jiang, Lei Shu, Jianwei Niu, Han-Chieh Chao, "Management And applications of trust in Wireless Sensor Networks: A survey", Journal of Computer andSystem Sciences, vol. 80, pp. 602-617, 2014.

[11] Thiruppathy Kesavan, Radha krishnan, S, "Secret Key Cryptography based Security Approach for Wireless Sensor Networks", IEEE International Conference onRecent Advances in Computing and Software Systems (RACSS), pp. 185 – 191, April 2012.

[12] Anand kumar K.M, Jaya kumar C , Arun Kumar P , Sushma M and Vikraman R, "Intrusion detection and prevention of node replication attacks in Wireless body area sensor network", International Journal of Ubiquitous computing, vol.3, no.3, pp. 1-10, July 2012

[13] G.Edwin Prem Kumar, Titus.I, Sony.I.Thekkakara, "A comprehensive overview on Application of Trust and Reputation in Wireless Sensor Network", Procedia Engineering, vol.38, pp.2903-2912, 2012.

[14] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar," SPINS: Security protocols for Sensor Networks", Mobile Computing and Networking, vol.8, pp. 521-534, 2002.

[15] Rodrigo Román, M. Carmen Fernández-Gago, Javier López, "Featuring Trust and Reputation Featuring Trust and Reputation Management Systems for Management Systems for Constrained Hardware Devices", in Proc. International Conference on Autonomics'07, 2007.

[16] Chithra Selvaraj, Sheila Anand, "A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks", Computer Science Review, vol. 6, pp. 145-160, 2012.

[17] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys and Tutorials, vol.14, no.2, pp. 279-298, 2012.

[18] A.Josang, R.Ismail and C.Boyd, "A Survey of trust and reputation systems for online service provision", Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[19] J.H.Cho, A.Swami and I.R.Chen, "A survey of trust management in mobile ad hoc networks", IEEE Communications and Surveys Tutorials, vol. 13, no.4, pp. 562-583, 2011.

[20] T.Grandison and M.Sloman, "A survey of trust in internet applications", IEEE Communications and Surveys Tutorials, vol. 3, no.4, pp. 2-16, 2009.

[21] Xiaoyong Li, Feng Zhou ; Junping Du, "LDTS: A Lightweight and Dependable Trust

System for Clustered Wireless Sensor Networks", IEEE Information Forensics and security,vol.8, no.6, pp.924-935, 2013.

[22] T.P.Rani, C.Jaya Kumar, G.Divya, "Trust aware Wireless Sensor Networks", in Proc. IEEE International Conference on Computing and Communications Technologies ICCCT'15, Feb 2015.

[23] Guoqiang Mao, Baris Fidan, Brian D.O, Anderson, "Wireless sensornetwork localization Techniques", Computer Networks, vol. 51, pp. 2529-2553, 2007.