Enhanced Beta Trust Model for Identifying Insider Attacks in Wireless Sensor Networks

Geetha V[†]

Department of Information Technology, National Institute of Technology, Karnataka, Surathkal

K. Chandrasekaran

Department of Computer Science and Engineering, National Institute of Technology, Karnataka, Surathkal

Abstract
Wireless sensor networks (WSN) are more prone to insider and outsider attacks as the sensor nodes are deployed in open environment for collecting data. The traditional cryptography based security mechanisms such as authentication and authorization are able to sort out issues of outside attacker, but they are not effective against insider attacks. Trust based approaches are used to defend against insider attacks in wireless sensor network. A trust model provides a way to quantify the trustworthiness of a sensor node. Watchdog is a popular mechanism to collect the information regarding the behavior of nodes. The existing trust models are having vulnerabilities for insider attacks in wireless sensor networks. In this paper, we discuss several security vulnerabilities in a Beta trust model for identifying insider attack and then propose countermeasures for defending against insider attacks in wireless sensor networks.

Key words:
Trust model, Insider attack, Wireless Sensor Network

1. Introduction

Traditional cryptographic techniques such as authentication and authorization can provide security with data integrity, confidentiality, authentication, and authorization. Along with these four security requirements wireless sensor network further requires to ensure availability, non-repudiation and data freshness. The attacks in WSN can be classified as outsider attacks and insider attacks. Outside attacks are defined as attacks from nodes which do not belong to a WSN and inside attackers are defined as the nodes which belongs to WSN and but behave in unintended or unauthorized ways. Inside attacker can disrupt the network by dropping, modifying or misrouting the data packets. Traditional cryptographic techniques provides mechanisms for defending against outsider attacks and cannot completely defend insider attacks. This is a serious issue in application like military, fire detection and other critical applications of industry etc.

Trust mechanism is used in other networks such as social network, e-commerce, p2p and ad hoc networks and provided effective results in identifying various kinds of attacks [1, 2, 3, 4]. The distributed nature of wireless sensor network insists on trust mechanism to a distributed in nature for evaluating, storing and updating the trustworthiness of other nodes based on trust model. In general, trust mechanism has following stages (i) Monitoring behavior of node (ii) Trust calculation based on observed behavior (iii) Attacker detection based on trust value and (iv)Trust update. In order to monitor the behavior of sensor node watchdog mechanism is popularly used in wireless sensor network. The watchdog keeps track of the number of packets sent to neighbor node and monitors whether the neighbor node has forwarded the packet towards sink or not. Based on the trust model such as Beta trust model [5] or Entropy trust model the trust is calculated by considering the collected information from watchdog. If the trust value of the neighbor is not above some threshold value, the node will be considered as inside attacker. A node selects its neighbor for forwarding a packet based on its trust value.

In wireless sensor network, the packet drops are common due to environment conditions. It is also possible that an attacker can simply drop the packet purposefully. So it is very difficult to identify whether a packet drop is due to an attacker or from contention or noise. If the drop was due to noise or contentions over a short period of time and if the node is falsely detected as malicious, then the service of the benevolent node which has been falsely identified as an attacker in the network, is not utilized with full capacity in the network. As a result of this fact, no trust models can completely prevent insider attack.

Beta trust model is the one of the popular trust model which has proven good results in other areas of network such as social network, ad hoc network [11] and P2P network etc. Our goal in this paper is to demonstrate how Beta trust model is vulnerable for insider attacks. The trustworthiness of a node can be calculated based on direct trust and indirect trust. Indirect trust calculation helps to converge the trust calculation faster. This approach is useful when nodes are mobile in the network. Since we are assuming the static WSN network deployed in an environment, in this paper, we are focusing on analysis of direct trust calculation.

Manuscript received August 5, 2013
Manuscript revised August 20, 2013

Rest of the paper is outlined as follows. Section 2 gives the background details about routing and trust calculation. Section 3 briefs about Beta trust model. In section 4, we explain the vulnerabilities of Beta trust model against inside attacker. Section 5 explains our proposed work along with the experimental results and discussion. The paper is concluded in section 6.

2. Background

In this section we discuss about the routing and packet forwarding, insider attacks, watchdog mechanism and trust calculation in wireless sensor networks.

2.1 Routing and Packet Forwarding

The sensor nodes senses the phenomena in environment and sends the data to sink node on multihop routing. We assume that CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used for wireless channel in WSNs [6]. After sensing the phenomena the node forwards the packet to next neighbor node based on its trust value. Marti et al [8] introduced a monitoring mechanism known as watchdog to identify misbehaving nodes in wireless ad hoc networks. In their approach, each sensor node has its own watchdog that monitors and records its one hop neighbor's behaviors such as packet transmission.

Let SR be the source node which would like to report its collected information to sink node BS. The routing protocols are used to form the routing path from SR to BS. A node in WSN contains a set of neighbor nodes. Let NB is the neighbor set of an intermediate node i in the routing path. The node i also maintains a set of neighbor nodes which are towards the sink node so that the node i can forward the packet. The node i selects a node in Forwarding Set based on highest trust value. Forwarding set is a subset of Neighbor set.

Consider the scenario as shown in figure 1. Source node SR has three intermediate nodes F, G, H as intermediate nodes in the path towards base station BS. To forward packets to BS, node SR first chooses a node F from its forwarding set as the next hop and sends the packet to F. Then SR starts monitoring F's behaviors. The SR overhears the packet forwarded by F to G and gets confirmed that the packet is forwarded to G. The watchdog in the node SR considers the operation as 'successful'. If SR does not get the ACK message from F, SR retransmits the packet up to a pre-determined number of times. If SR does not get the ACK message even after the maximum retransmission, then SR discards the packet. This operation is considered as "failure' in watchdog of SR. The ‘success’ operation observed contributes towards the increase in trust value of F and the 'failure' operation contributes towards the decreased value of trust of F in SR. As the WSN is distributed, we consider that every node runs the watchdog to monitor the behavior of its neighbors. If the neighbor’s failure increases above the threshold value, SR treats F as an attacker.

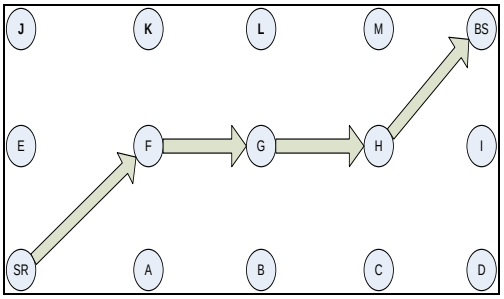

Figure 1: Routing in Wireless Sensor Network

2.2 Insider Attacks in WSN

To defend against outside attackers, we assume that our WSN is equipped with cryptography based authentication and authorization [5]. Inside attacker can damage our network stealthily as they can initiate dos attacks, packet drop attacks etc without getting noticed by cryptographic techniques. The dropping of critical packets related to data and routing protocols disrupts the network in large way. Packet drop attacks are difficult to identify with cryptographic technique as it’s difficult to distinguish between a packet drop due to insider attack or due to contention or noise. If inside attacker are positioned near sink node BS then, the network performance degrades as packet delivery rate decreases. There are several types of packet drop attacks such as blackhole, gray hole attack and on-off attack [3, 7]. **No attack:** Forward all packets; **Blackhole attack:** Drop all packets; **Grayhole attack:** Drop (specific) packets randomly; and **On-off attack**: drop all or some portion of packets periodically. Compared to blackhole attack, it is harder to detect grayhole attack and on-off attack due to their complicated attack patterns. Moreover, packet drop attacks have evolved to intelligently drop packets by exploiting inside knowledge about network and security mechanism to avoid being detected [3]. For this reason, in this paper we mainly focus on inside attacker's packet drop attacks.

2.3 Watchdog Mechanism and Trust Calculation

Watchdog mechanism is a node behavior monitoring system. Every sensor node monitors the behavior of its neighbor node based on watchdog system. The nodes are set in promiscuous mode and watchdog keeps track of whether the neighbor node has further forwarded the packet in the line of path towards sink node or not. Based on the count of number of successful forwarded packet and number of unsuccessful packets forwarded by the neighbor

node, the trust value can be built to monitor the behavior of it. In general, building trust value in trust mechanism has following stages.

(i) Monitoring behavior of node

Each sensor node monitors and records its neighbor's behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. Watchdog is a monitoring mechanism popularly used in this stage.

(ii) Trust calculation based on observed behavior

Trust model defines how to measure the trustworthiness of a sensor node. Yu et al [3] introduced several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game theoretic approach and Fuzzy approach. Since the Bayesian trust model with beta distribution is the widely used trust model, we are focusing on Beta trust model and its vulnerability to insider attack in WSN.

(iii) Attacker Detection based on trust value

Normally, a threshold value is used to detect whether a node is malicious or not. If the trust value is greater than threshold value, then the node is considered as normal node, else it is identified as an attacker.

(iv)Trust update

Based on occurrence of event the trust value is updated.

3. Beta Trust Model for WSN

In [5] Josang and Ismail developed the beta reputation system for electronic markets, based on distribution by modeling reputation as posterior probability based on past experiences. They used the beta probability density functions to combine feedback and derive reputation ratings. The advantages of the beta reputation system are flexibility and simplicity, as well as its foundation on the theory of statistics. The certainty of the trust calculation is defined by mapping the beta distribution to an opinion, which describes beliefs about the truth of statements. In this section we discuss calculation of trust by existing Beta trust model and associated trust update procedure.

3.1 Monitoring Behavior of a Node

Watchdog is used to observe the behavior of neighbor node. In Figure 1, if a node F forwards a packet to node G and if node G further forwards the packet to node H then the observation of node G forwarding packet to node H is observed by the watchdog in node F. This scenario is considered as "successful" operation. If node G does not forward the packet sent by node F then node F considers the operation as "failure". The node F also considers the operation as "failure" if it does not receives any ACK from node G.

When a node is observed to forward the packet 's' times and drops the packet 'f' times, the Beta trust model will assign trust value T(0<= T<=1) to this node using formula

$T = (s+1)/(s+f+2)$ ---------- (1)

In (1) the numerator has '+1' and denominator has '+2' which indicates that at least two trails were observed out of which one was 'successful' and other was 'failure' according to Laplace law. This concept makes the initial trust value for each node as 0.5.

3.2 Trust Update

The watchdog is used to collect the information over a period of time. Since trust update for every single packet is a tedious job and needs lot of energy the trust values can be updated periodically, by collecting the data from watchdog for an interval of time unit t.

If s_t and f_t are the number of successes and failures observed in unit time 't', then the parameters 's' and 'f' can be updated as follows:

$$s^{new} = s^{old} + s_t$$
$$f^{new} = f^{old} + f_t \quad \text{----------} \quad (2)$$

Since, the WSNs are small devices with limited resources the space for storing the value of s^{new} and f^{new} may run out of space and come back to initial value zero. The oldest information can be given less priority while calculating trust value. This concept is called 'aging' and a parameter β is used to update the trust value as follows.

$$s^{new} = s^{old} * \beta + s_t$$
$$f^{new} = f^{old} * \beta + f_t \text{ where } \beta \in [0,1] \quad \text{----------} \quad (3)$$

3.3 Attacker Detection

A threshold value θ_T is used to identify the inside attacker. The trust value T obtained by observation is compared with θ_T as follows:

If $T >= \theta_T$ then the node is a normal node.

If $T < \theta_T$ then the node is a malicious node ----- (4)

Figure 2 shows the behavior of Beta trust model for 100% success and 50% success observation for every unit interval of time (t=20). The trust value gradually increases up to 1 if there are consecutive successes & decreases towards 0 for consecutive failures.

4. Vulnerabilities in Beta Trust Model for Insider Attacks in WSN

We now examine the security weakness in Beta trust model for identifying insider attacks. Vulnerabilities can occur in

the stage of data collection as ambiguous collision, receiver collision and limited transmission power [9].

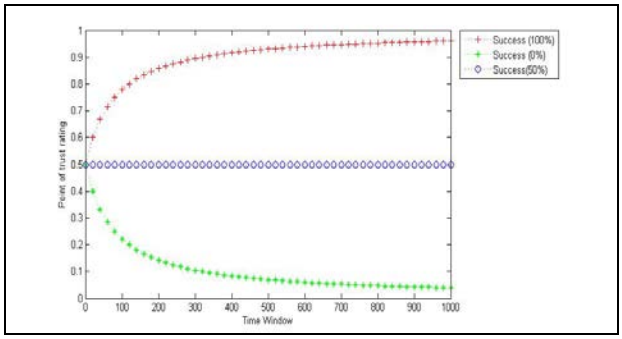

Figure 2: Behavior of Beta Trust Model

4.1 Vulnerability in the Inside Attacker Detection Stage

In this stage, a node is classified as either trustful or distrustful. The value of the trust threshold (θ_T) that is used for such classification in the single most important parameter at this stage. A low θ_T will misclassify attackers as trustful nodes and a high θ_T will cause unnecessary false alarm. θ_T must be carefully determined to maximize attacker detection rate and minimize false alarm rate.

The Cho et al [9] explains how the detection of θ_T by an attacker leads to dropping of packets, without being detected as malicious. We can also observe that the Beta trust model is not able to detect selective forward and on-off attacks as the equation (1) considers total history for trust calculation. The recent drop behavior doesn't gets caught immediately, in case of equation (1).

For example, the initial value of T is 0.5 in equation (1) indicates that the node is yet to start the communication. If θ_T is kept as static and θ_T = 0.5 then inside attacker can drop nearly 50% of packets in an unit interval of time and still not get identified as malicious node. If θ_T is kept as θ_T > 0.5 for example θ_T = 0.75 then most of the nodes get identified as inside attack as the initial value of trust T gets set as 0.5, based on equation (1).

4.2 Rate of Packet Drop

If θ_T =0.75, and if attacker knows or assumes this value, then after certain numbers of initial successful forwarding (to build a high trust value) the attacker can drop a considerable number of packets consecutively without bringing its trustworthiness to below θ_T. For example, with s=1000 previous successful forwarding the next 334 packets can be dropped without being detected as an attacker by the Beta trust model.

In general, if s^{old} is the given number of successful operation, an attacker can find the number of packets which it can drop and still maintain condition of θ_T can be found as follows from equation (1).

$$d= (s^{old} + 1 - (\theta_T * (s^{old} + 2))) / \theta_T \quad \text{---------- (5)}$$

where d is the total number of packets which can be dropped by an insider attacker, along with maintaining the condition of θ_T. The goal of trust model must be to reduce the value of 'd' as much as possible.

4.3 Consecutive Failures

We believe that handling consecutive failures approximately improves the early detection ability of a trust model because of two reasons. First, most packet drop attacks such as blackhole, grayhole and on-off attack generate a certain degree of consecutive failures. Second, if the size of consecutive failures 'n' grows, our belief that the node generating the 'n' consecutive failures is not a normal node. (that is, it is an attacker or a faulty node) will also grow based on the following probabilistic reasoning.

Meanwhile we observe that beta trust model does not address consecutive failures. Consider the two scenarios observed in which one scenario shows alternate success and failures of 20 operation and other scenario with continues 10 successes and 10 failures. Even though the trust calculated by equation (1) is same in both cases, the chance of failure in case of second scenario is more compared to the first one. Moreover, it is often assumed that inside attackers launch attacks after they develop high trust to avoid being easily detected [4, 9].

Chen et al [10] provides a mechanism to update trust value in order to reduce the trust when there are consecutive drops as follows.

$$s^{new} = s^{old} * \beta + s_t$$
$$f^{new} = f^{old} * (1-\beta) + f_t \text{ where } \beta \in [0,0.4] \quad \text{---------- (6)}$$

The issue in this model is, the trust value takes maximum value as 0.7 and not beyond that. The more weight is given to failure detection. So the trust value decreases as the number of failure increases.

5. Proposed Work: Counter Measures and Experiments

The issues related to detection of insider attacks in wireless sensor networks using Beta trust model and its effects are briefly discussed in section 4. This section, proposes the countermeasures and related experimental results.

5.1 Countermeasure for Initialization of Trust Value

In wireless sensor network, the nodes towards sink node forward the packet to sink node. Hence, they play a major role in establishing routing path compared to the node

which simply forwards the packet. For example, consider the scenario shown in Figure 3.

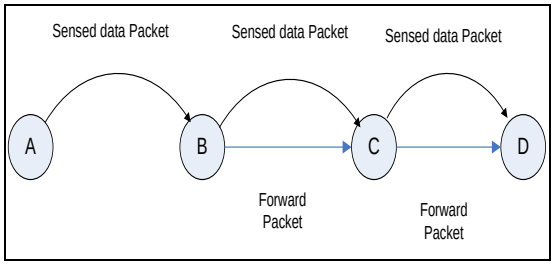

Figure 3: Forwarding and Non-Forwarding Nodes

The node A, B, C and D are forming a communication path. Every node sense some data and forward it to next node towards sink. Node D is the sink node. In case of node B, it sends its data packet to node C as well as forwards the packet received from node A. Here, the destination or sink node is D. In this scenario node B has to consider node C s trust compared to node A. So based on this condition we can classify the neighbor nodes as Forwarding Node (FN) or Non-Forwarding Node (NFN). Apply strategy for identifying insider attack to Forwarding Node set. This reduces the false rate of inside attacker detection based on θ_T, as inside attackers are checked on active nodes such as FN's. We can have initial values for FN's and NFN's separately as follows.

T_{init} = (s+1)/(s+f+2) for NFNs

or

T_{init} = (s+3)/(s+f+4) for FNs ---------- (7)

If a node is an active member for forwarding the packets, then we assume that prior to the process around 75% of operations were successful. This makes θ_T value for normal node behavior to be in the range (0.75 to 1).

Simulation experiment is conducted using MATLAB. Two node scenario is considered where a node i sends the packets to node j. The simulation is run for three different cases. (i) node j forwards all the packet sent by node i successfully (ii) node j forwards only 50% of the packets sent by node i in a period of time and (iii) node j drops all the packets sent by node i. Figure 4 shows the trust values for node j which is a Forwarding Node (FN) for node i with 100%, 0% and 50% success in each time interval (t=20). We can observe that since θ_T =0.75, only node with success rate of 100% gets detected as normal node. Even a node which behaves with 50% success in each time interval gets detected as insider attack as its trust value is below θ_T.

5.2 Countermeasure for Issues with Packet Drop Rate and Consecutive Drops

To reduce the value of 'd' shown in equation (5) one has to consider the consecutive drops as a parameter in the trust value. The trust value must decrease as the number of consecutive drops increases. We propose a new update procedure as follows: The trust value must increase slowly when there is consecutive successes. The trust value must drop fast for consecutive failures. Our approach is to put a penalty on number of successful cooperation based on consecutive drops. We consider the recent behavior to measure the trustworthiness.

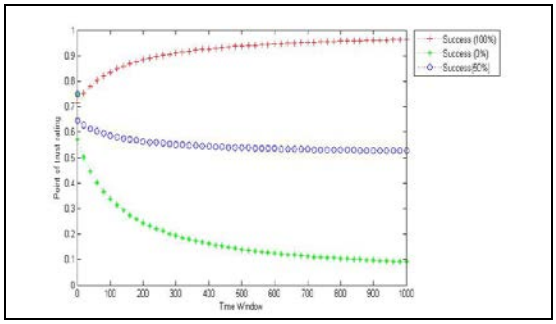

Figure 4: Behavior of Beta Model based on equation (4)

Proposed algorithm 1

1. $F_{penalty}$=1;
2. β=0.98;
3. $T_{recent}=s_t/(s_t+f_t)$;
4. if $T_{recent} < \theta_R$ then
5. **begin**
6. $F_{penalty} = F_{penalty} * 2$;
7. $s^{old} = s^{old} / F_{penalty}$;
8. **end**
9. if $s^{old} < 0.1$ then $F_{penalty}=1$;
10. $s^{new} = s^{old} * \beta + s_t$;
11. $f^{new} = f^{old} * \beta + f_t$;

// Trust Calculation

12. $\mathbf{T_{total} = (s^{new} + 1) / (s^{new} + f^{new} + 2)}$;

The proposed algorithm 1 considers the trust value based on recent observation as $T_{recent} = s_t/(s_t + f_t)$. If the value of recent trust is less than threshold value θ_R then the penalty is put on the goodness of nodes behavior by reducing the value of successful interactions s^{old} as $s^{old} = s^{old} / F_{penalty}$. Now the question is what must be the value of penalty. We consider exponential reduction by increasing the value of $F_{penalty}$ by 2 for every low unsuccessful rate observed in an interval of time. At end the s^{new} and f^{new} are updated based on normal beta trust model with aging factor β.

Proposed algorithm 2

1. $F_{penalty}$=1;
2. β=0.98;
3. $T_{recent}=s_t/(s_t+f_t)$;
4. if $T_{recent} < \theta_R$ then
5. **begin**
6. $F_{penalty} = F_{penalty} * 2$;
7. $s^{old} = s^{old} / F_{penalty}$;
8. **end**
9. if $s^{old} < 0.1$ then $F_{penalty}=1$;
10. $s^{new} = s^{old} * \beta + s_t$;
11. $f^{new} = f^{old} * \beta + f_t$;

// Trust Calculation

12. $\mathbf{T_{total} = (s^{new} + 3) / (s^{new} + f^{new} + 4)}$;

In proposed algorithm 2 the node is considered as a Forwarding Node (FN) hence the trust value T_{total} is calculated based on equation (7) as follows:

$T_{total} = (s^{new} + 3) / (s^{new} + f^{new} + 4)$;

Simulation experiments are conducted using MATLAB. Two node scenario is considered where a node i sends the packets to node j. The simulation is run for time interval 1500 units. The watchdog is updated for every time interval (t=20). The node j forwards the packets sent by node i up to time interval 1000 units. After that the node j drops the packets as it has achieved high value of trust by this time. Two different packet dropping patterns are considered. (i) Dropping all the packet (Sink hole attack) and (ii) Dropping 50% of the packets (selective forwarding/on-off attack).

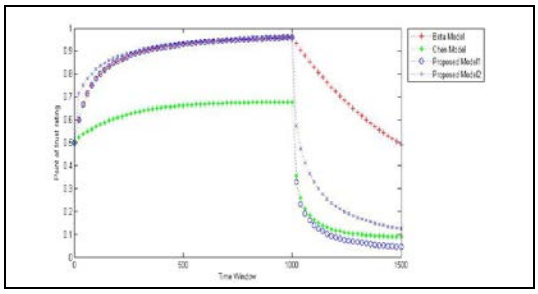

Figure 5: Behavior of Trust Models with consecutive drops after obtaining high trust value.

For analysis we have considered beta trust model, beta trust model with enhancement proposed by Chen et al, proposed algorithm with penalty for misbehavior is considered as proposed model 1 and initialization value based on Forwarding Node proposed in equation (6) along with penalty for misbehavior is considered as Proposed Model 2 whose results are shown in Figure 5 and 6 . Figure 5 shows the result of 100% packet drop after obtaining high trust value and figure 6 shows the result of 50% packet drops after obtaining the high trust value.

6. Conclusion

The detection of insider attacks in wireless sensor networks is a crucial task. Trust models have provided good results for identifying insider attacks. The Beta trust model is the widely used trust model in various networks due to its simplicity. However, the existing Beta trust model is having vulnerabilities for insider attacks in wireless sensor network. In this paper, we have discussed various vulnerabilities of Beta trust model for insider attack and we have proposed the countermeasures for these vulnerabilities. One major issue is about initialization of trust value, which can be solved by initializing the forwarding and non-forwarding node's trust value separately. We have proposed the method for identifying contiguous or selective packet drops by putting penalty for such behavior. The enhanced proposed models shows better results compared to Beta trust model.

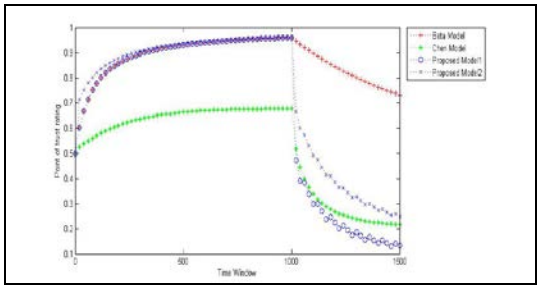

Figure 6: Behavior of Trust Models with 50% packet drops for unit interval of time, after obtaining high trust value.

Time in units	Trust Value Based on Beta Trust Model	Trust Value Based on Chen Trust Model	Trust Value Based on Proposed Model 1	Trust Value Based on Proposed Model 2	Variation of trust value in Beta Model	Variation of Trust Value in Chen Model	Variation of Trust Value in Proposed Model 1	Variation of Trust Value in Proposed Model 2
980	0.95985138	0.67732472	0.95985138	0.96207180	-----	-----	-----	----
1000	0.96048159	0.67744918	0.96048159	0.96264580	0.0006	0.0001	0.0006	0.0006
1020	0.93240829	0.35661118	0.32937248	0.57259805	-0.0281	-0.3208	-0.6311	-0.3900
1040	0.90543729	0.25824708	0.23102885	0.47398455	-0.0270	-0.0984	-0.0983	-0.0986
1060	0.87951011	0.21233066	0.18930991	0.41192475	-0.0259	-0.0459	-0.0417	-0.0621
1080	0.85457230	0.18375975	0.16084910	0.36508211	-0.0249	-0.0286	-0.0285	-0.0468
1100	0.83057310	0.16398586	0.14019617	0.32847742	-0.0240	-0.0198	-0.0207	-0.0366

Figure 7: The variation of trust value when the node j starts dropping packets 100% at time 1000 units.

Reference

[1] Denis Treek, "Trust Management in the pervasive Computing era", IEEE security & Privacy, Vol 9,No.4, July 2011, pp 52-55.

[2] Vijay Vardharajan, "A note on Trust Enhanced Security", IEEE Security & Privacy, Vol 7, Issue 3, May/June 2009, pp 57-59.

[3] Yanli Yu, Kequi Li, Wanlei Zhou and Ping Li, " Trust Mechanisms in Wireless Sensor Networks :attack analysis and Countermeasures, " Journal of Network and Computer Applications, Elsevier, 201, Vol 35, pp 867-880.

[4] Javier Lopez, Rodrigo Roman, Issac Agudo, and Carmen Fernandez Gago, "Trust management systems for wireless sensor networks: Best practices, "Computer Communication Vol 33, 2010,pp 1086 -1093.

[5] A. Jasong and R. Ismail, "The Beta Reputation System", In Proc. of the 15th Bled Electronic commerce Conference, June 2002.

[6] Azahdeh Fandi et al, "Comprehensive Evaluation of the IEEE 802.15.4 MAC Layer Performance with Retransmissions, "IEEE Transactions on Vehicular Technology, Vol 59, No. 8, October 2010, pp. 3917 - 3932.

[7] Yan (Lindsay Sun, Zhu Han, and K.J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks IEEE Communications Magazine, Vol 46, Issue 2, 2008, pp 1-119.

[8] Sergio Marti, T. J. Giuli, Kelvin Lai and Mary Barker, "Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks", In Proc. of International Conference on Mobile Computing and Networking (MobiCom), 2000, pp 255-265.

[9] Youngho Cho, Gang Qu and Yuanming Wu, "Insider Threat against Trust Mechanism with watchdog and defending Approaches in Wireless Sensor Networks" IEEE Computer society 2012, pp 134-141.

[10] Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao Agent-based Trust Model in Wireless Sensor Networks 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007) PP 119-124, July 30 - Aug 1, 2007 Qingdao, China.

[11] Zuhao Liu, Li Yu, Wei Cheng and Ke Wang, A Cooperative Recommendation Trust Model for Ad Hoc Networks, 6th International ICST Conference on Communications and Networking in China, 17-19 Aug.2011, pp 319-323.

Geetha.V obtained her Bachelor of Engineering degree from Mangalore university in 1999. She has obtained her M.Tech degree in Computer Science and Engineering from VTU, Belgaum in 2004. Currently she is pursuing her Ph. D. in Department of Computer Science Engineering, National Institute of Technology Karnatka, Surathkal (NITK). She is also working as Assistant Professor in the Department of Information Technology, NITK, Surathkal since from year 2008. Her area of interest is Computer Architecture and Wireless Sensor Networks.

Dr. K. Chandrasekaran is currently working as professor in the department of Computer Science and Engineering and Dean of Reasearch and Consultancy at National Institute of Technology Karnataka Surathkal. He is having More than 25 years of teaching experience. His research interests includes Distributed Computing, Computer Networks and Cloud Computing. He has more than 100 research publications in reputed or peer reviewed journals and International Conferences. He was visiting Fellow/researcher/prodfessor at various higher learning Institutes in India and abroad which includes LMU UK, AIT Bankok and UF USA.