Trust-Based Hierarchical Routing Protocol for Wireless Sensor Networks

Article · June 2015

CITATIONS
0

READS
186

5 authors, including:

Yamuna Devi C R
Dr. Ambedkar Institute of Technology
15 PUBLICATIONS **26** CITATIONS
SEE PROFILE

SH Manjula
UVCE, Bangalore University
94 PUBLICATIONS **204** CITATIONS
SEE PROFILE

Lalit M Patnaik
Indian Institute of Science
838 PUBLICATIONS **8,709** CITATIONS
SEE PROFILE

International Journal of Information Processing, 9(1), 101-112, 2015
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Trust-Based Hierarchical Routing Protocol for Wireless Sensor Networks

Yamuna Devi C R[a], Saishiva K[a], Sunil Kumar[a], S H Manjula[a], K R Venugopal[a], L M Patnaik[b]

[a]Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India. Contact: yamuna.devicr@gmail.com

[b]Indian Institute of Science, Bangalore, India.

Network Lifetime is an important issue in Wireless Sensor Networks. It depends on many factors like the amount of data to be communicated, number of nodes in the network and initial energy of the sensor nodes. This paper proposes a novel routing protocol by name Trust-Based Hierarchical Routing (TBHR) protocol for multi-hop hierarchical wireless sensor network. The proposed protocol is based on trust evaluated for every sensor node in the network. Trust of a sensor node comprises of components derived from communication and social networks. Trust of a sensor node depends on the residual energy of the node and the number of transactions it has with its neighbors and its cluster head. The proposed protocol has two fold benefits. First it allows more number of nodes in the network to participate in transmission to balance energy in the nodes and thus improves the network lifetime. Second it ensures better packet delivery ratio though the number of untrustworthy nodes increases in the network. The data packet is flooded in the network by the source node when the number of trustable nodes in the network falls below 35 % of total nodes in the network. Flooding achieves optimum packet delivery ratio in the network. The same facts are verified by simulation results by analyzing the factors sensor node trust, network lifetime and delivery factor.

Keywords : Clusters, Malicious Node, Trust, Wireless Sensor Networks.

1. INTRODUCTION

Wireless Sensor Network consists of tiny self-powered sensor nodes which can sense, process and transmit data to other nodes in the network [1]. It is composed of a large number of spatially distributed autonomous sensor nodes to cooperatively monitor physical and environmental conditions, such as pressure, temperature, vibration, sound, and pollutants. The function of sensor node deployed in the wireless sensor networks, is to sense the information and transmit, or, forward the information to the sink node. The base station or the sink node is connected to the source nodes through one-hop or multi-hop routing. Networks with multi-hops are either star connected, or, clustered. Applications that require efficient data aggregation are natural candidates for clustered networks.

While sensor nodes are popularly used for various monitoring purposes such as wild animal tracking, weather monitoring and for battlefield surveillance, they have severely restricted resources such as energy, memory, and computational power. In addition to the restrictions on resources, the sensor nodes need to follow security implications. Further, wireless environments give more design challenges to network functioning due to inherently unreliable communication. But some applications require a combination of wired and wireless communication technologies [2].

Sensor networks usually perform unattended operations. So, it is important to design network protocols in such a way that network function is not affected by the presence of compromised or malicious nodes in the network. The sensor nodes sometimes perform malicious attacks such as packet dropping or packet modifications. The normal operation of a wireless

sensor network is disrupted, when the sensor nodes are compromised. The lifetime of sensor node depends on the energy consumed at the sensor nodes for different operations like information sensing and packet transmission by the node. Wireless sensor networks aim at smaller size, decreased cost and increased battery lifetime of the sensor nodes. Sensor node energy consumption is considered in two dimensions: low energy consumption and efficient energy consumption. For all the necessary operations of the sensor node, energy consumption has to be at minimal level. Energy consuming activities have to be reduced, for efficient energy consumption.

Autonomous operation of the sensor nodes in the sensor network is one of the major requirements as nodes are deployed in strategic locations where human intervention is not easy. Wireless sensor network must be fault tolerant and robust to adapt to failure of some of the nodes in the network. Specific applications of wireless sensor networks like closed loop regulatory systems are extremely delay sensitive and require communication in wireless sensor network to be predictable and real time guaranteed. Data aggregation in the same sensor, or, among a group of sensors is another method to minimize number of packets communicated in the network to increase energy efficiency of wireless sensor networks.

In networks with higher node density, large numbers of sensor nodes are deployed in the network, nodes are very close to each other. Hence, multi-hop communication in sensor networks consumes lesser power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in several applications of networks. Multi-hop communication effectively overcomes some of the signal propagation effects experienced in long-distance wireless communication.

Based on the network structure, routing techniques in wireless sensor networks can be classified as flat routing and hierarchical routing techniques. In flat routing, all the nodes have equal capabilities and functionalities. Sequential assignment Routing and Directed Diffusion are examples of flat routing techniques. Sensor nodes are divided into clusters and each cluster has a cluster head node with special functions in hierarchical routing. LEACH [3] and HEED are Time Division Multiple Access (TDMA) based hierarchical routing techniques. Multipath routing ensures reliability and timely delivery of data from source to destination node in a network. Fault tolerant routing protocols provide robust routing techniques that are less affected by failure of links among nodes and nodes themselves.

Trust is one of the main mechanisms to provide security [4] in the operation of wireless sensor network. Trust is a multidimensional, complex, and context dependent concept. To calculate trust of a node and identify nodes as malicious, several parameters are considered. Trust management in sensor network includes key design issues such as trust composition, trust aggregation and trust formation. Intimacy, honesty, energy and unselfishness of sensor nodes are considered as the components of trust. Aggregation of trust of sensor nodes in hierarchical networks is done by the cluster head nodes. Trust formation is done based on communication as well as quality of service factors.

Contribution: The battery lifetime of a sensor node is a very important factor in deciding the lifetime of a network. Reliable transmission in communication is another important quality of a good sensor network. A hierarchical routing protocol for Wireless Sensor Networks is proposed to improve the network lifetime and the packet delivery factorin the network using trust of the nodes. Trust of a sensor node is formed based on the interaction of the node with its neighbors and its residual energy.

2. RELATED WORK

Any work is incomplete without the knowledge of past developments in the same field. This section describes some the previous works

that are based on hierarchical wireless sensor networks, routing protocols and trust management in wireless sensor networks.

Duan *et al.,* [6] propose a trust based secure routing protocol to resist various attacks in wireless sensor networks. A combination of trust metric and QoS metric are used as routing metric to improve security aspects of the performance of a dense network. Aivaloglou and Gritzalis [7] propose a hybrid trust management model to uniformly support the needs of nodes with different roles and capabilities using the knowledge of network topology and the information flows. The trust establishment is done based on certificate based and behaviour based approaches on common evaluation processes and metrics. The results and analysis of simulations show the effectiveness in managing the trust relationships between nodes and clusters in the network.

Liu *et al.,* [8] consider the security of geographic routing used in ad-hoc and wireless sensor networks. A location verification algorithm is proposed to address the attacks of false location information in networks. Another algorithm is proposed for trust-based probabilistic multi-path routing to defeat attacks on geographic routing. Possible attacks and security issues in network are directions for future work. In the work [9], a new lightweight Group-based Trust Management Scheme (GTMS) for wireless sensor networks that employs clustering is proposed. The approach reduces the cost of trust evaluation for sensor nodes. The theoretical as well as simulation results show that the scheme demands less memory, communication overheads and energy as compared to the current state-of-the-art trust management schemes. Furthermore, GTMS enables us to detect and prevent malicious, selfish, and faulty nodes.

Zhang *et al.,* [10] proposes a trust-based defending model against false routing information, selective forwarding and Sybil attack in wireless sensor networks. A combination of energy, routing cost and trust are used in next hop of routing. The simulation results show that the proposed model has advantages of packet delivery ratio and network lifetime over the existing models. In paper [11], the authors focus on pre-distribution schemes well-adapted for homogeneous networks to identify generic features that can improve some of the metrics for lightweight key management solutions for wireless sensor networks. The challenges in the area and future research directions are discussed in this paper.

The differences between security and trust in wireless sensor networks is discussed in [12]. The paper concludes that data trust and communication trust have to be combined to infer the total trust in the network. A survey of trust models in different network domains is given in paper [13]. The authors in [14] propose a novel hierarchicaltrust managementscheme that minimizes communication and storage overheads. This scheme takes into account direct and indirect or group trust in trust evaluation as well as the energy associated withsensor nodesin service selection. The authors consider the dynamic aspect of trust by introducing a trust varying function which could give greater weight to the most recently obtained trust values in the trust calculation.

Xia *et al.,* [15] proposed a subjective trust management model with multiple decision factors based on analytic hierarchy process theory and fuzzy logic rules prediction method. Factors like direct trust, recommendation trust, incentive function and active degrees are used to reflect trust relationship complexity. Experiments show that better network interaction quality, malicious node identification, trust dynamic adaptability, attack resistance and security enhancement is achieved in comparison with existing trust management models.

The concepts and properties of trust and derive unique characteristics of trust in Mobile Ad-hoc Networks are discussed in [16]. The resource constraints like computing power, energy, bandwidth, time and dynamics like topology changes, node failure, propagation channel

conditions are considered in managing trust. In [17], the authors study the effect of data forwarding and transmission path in the design of routing protocol for wireless sensor network. The parameters considered for analyzing the network performance are network lifetime, packet delivery rate and transmission latency.

Couto *et al.,* [18] presented the expected transmission count metric (ETX), which finds high-throughput paths on multi-hop wireless networks. ETX reduces the expected total number of packet transmissions in the network. A hybrid trust and reputation management scheme for wireless networks is proposed in [19]. Liu *et al.,* [20] consider the security of geographic routing used in ad-hoc and wireless sensor networks. The delivery of data packets to the destination node and increasing the lifetime of the network are of prime importance in most of the above works.

3. SYSTEM ARCHITECTURE

The cluster-based wireless sensor network considered in this paper has one base station and 50 sensor nodes. Four clusters, each cluster contains a cluster head and member sensor nodes in the corresponding geographical area are formed. Each of the sensor nodes in the network has a single receiver and a single transmitter unit. The cluster member sensor nodes are homogeneous. When the energy and resources required are considered, the cluster head needs more energy and resources compared to normal sensor nodes, as it has to forward the data of all its members. Hence the initial energy and transmission range of cluster head nodes are more than that of member nodes.

A sensor node forwards the sensed data to its cluster head and the cluster head then forwards the data to the sink or base station located in the network [4]. The selection of sensor nodes to forward the data to the base station is done by considering the Trust of the sensor nodes. The data gets routed through the forwarding node to other sensor nodes and the same factors apply to other sensor nodes, till the data reaches the base station.

3.1. Network Model

The graph model is used to analyze routing issues in wireless sensor networks. For a weighted directed graph *G(V, E, ω)*, the variable V stands for the set of sensor nodes in the network. E contains $V \times V$ edges that represents the connectivity of nodes. The weighted label ω) stands for metric used for measuring weights or distance between the nodes connected. For each (i, j) that belongs to E, the node i is the sender and node j represents the destination of information. A path ρ from vertex V_1 to vertex V_n is denoted by (V_1, V_n) equal to $(V_1, V_2, \ldots, V_n)$, consisting of *n-1* edges. The vertices V_2 to V_{n-1} represent intermediate vertices or forwarding nodes.

The trust management protocol for the given graph is conducted using periodic peer-to-peer trust evaluation for all the sensor nodes. The trust update interval is used to find the trust value of each sensor node in the network. The trust value of each sensor node is calculated considering the social trust and QoS trust components at every interval of time. Social trust of wireless sensors comprises of intimacy, honesty, privacy, centrality, and connectivity. QoS trust includes competence, cooperativeness, reliability, task completion capability, *etc.*,. The protocol is formulated such that it is generic and can take a combination of major social trust and important QoS trust metrics to form the overall trust metric. By considering the trust value of each sensor node, a trust worthy node is determined for forwarding data towards destination in the network.

The intimacy component of trust is considered for measuring closeness between sensor nodes based on interaction experiences and honesty is considered for measuring regularity or anomaly to measure social trust derived from social networks. Energy is chosen for measuring competence and unselfishness measures cooperativeness to indicate QoS trust derived from communication networks. The intimacy trust com-

ponent reflects the relative degree of interaction experiences between two nodes. The honesty trust component strongly implies whether a sensor node is malicious or not. Energy is an important metric in wireless sensor network since sensor nodes are extremely constrained in energy. Energy is used as a QoS trust metric to measure if a sensor node is competent in performing its intended function.

The trust management protocol is applied to a clustered wireless sensor network with static nodes. This network consists of heterogeneous sensor nodes with two different initial energy levels. The cluster heads are supplied with higher initial energy compared to initial energy of cluster member sensor nodes. A sensor node is more likely to become selfish when it has low residual energy. A cluster head consumes more energy than sensor nodes, as it has to forward the packets from all of its member nodes to the base station. After a sensor node is compromised, it consumes more energy to perform various attacks. On the other hand, a selfish node consumes less energy than an unselfish node as its selfish behavior is reflected by stopping sensing functions and arbitrarily dropping messages. The compromised or selfish nodes can perform various attacks including forgery attacks, dropping of packets, consuming a lot of energy without performing any functions. Thus, the only defense of the system is to avoid such attacks before a system failure occurs.

3.2. Trust Model

The peer-to-peer trust evaluation process considers social and QoS factors. Intimacy and honesty fall under social factors whereas energy and unselfishness are the QoS factors. The same hierarchy is depicted in Figure 1. The trust value the sensor node i evaluates towards sensor node j at time t, *Tij(t)*, is represented as a real number in the range of [1, 0] where trust value of 1 indicates complete trust, 0.5 is ignorance, and 0 indicates distrust.
Trust of node i, $T_{ij}(t)$ at instant t is computed by the following equations:

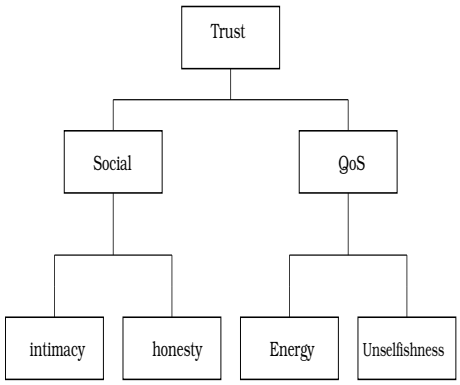

Figure 1. Components of Sensor Node Trust

$$T_{ij}(t) = T1 + T2 + T3 + T4 \tag{1}$$

T1, T2, T3 and *T4* in (1) are given by:

$$T1 = W_1 T_{ij}^{in}(t) \tag{2}$$

$$T2 = W_2 T_{ij}^{ho}(t) \tag{3}$$

$$T3 = W_3 T_{ij}^{en}(t) \tag{4}$$

$$T4 = W_4 T_{ij}^{un}(t) \tag{5}$$

where W_1, W_2, W_3 and W_4 represent the weight associated with the components intimacy, honesty, energy and unselfishness of the sensor node. The special case in which intimacy and honesty are equal and energy and unselfishness are equal is considered is represented by

$$W_1 + W_2 = W_3 + W_4 \tag{6}$$

So Eq. (1) can be rewritten as

$$Tij(t) = 0.5W_S + 0.5W_Q \tag{7}$$

W_S and W_Q are given by the following equations:

$$W_S = W_S oc[T_{ij}^{in}(t) + T_{ij}^{ho}(t)] \tag{8}$$

$$W_Q = W_Q oS[T_{ij}^{en}(t) + T_{ij}^{un}(t)] \tag{9}$$

where

$$W_{Soc} + W_{QoS} = 1. \tag{10}$$

The significance of each component of trust of a sensor node is as follows:

$T_{ij}^{in}(t)$: This term stands for intimacy *in* and indicates the level of interaction between the two nodes over the time interval. So, this measures the level of interaction experiences computed by the number of interactions between nodes i and j and any neighbor node of other nodes over the time period [0, t].

$T_{ij}^{ho}(t)$: The *ho* is the Honesty related to a node means the behavior of a node. That is, the node should perform all its intended functions like transmitting the packets, receiving the packets as well as forwarding the packets successfully. If the node is performing all the intended functions successfully, then the node is said to be honest node. But, when it creates nuisance over the network such as dropping of packets and performing attacks, then the node is considered as a dishonest node. So, determining a dishonest node in the network is an important task because it degrades the system performance and reduces the lifetime of the network. So, in order to avoid such a situation, determining the behavior of a node is essential.

$T_{ij}^{en}(t)$: Energy - *en* indicates the residual energy level of the node. The cluster head consumes more energy than the normal sensor node. The energy consumption rate is affected by the state of the node. It is lower when the node becomes selfish and higher when the node is compromised, because it takes more energy to perform the attacks. So, this measures the percentage of node is remaining energy so that in future it can perform all its necessary functions.

$T_{ij}^{un}(t)$: In the wireless sensor network system model considered, a node may become selfish to save energy. A selfish node may stop sensing data and drop packets it receives. An unselfish node may turn selfish at any trust evaluation interval t according to its remaining energy and the number of unselfish neighbors around. So, this component -*un* detects the selfish behavior of a node such as not faithfully performing sensing and reporting functions, data forwarding functions, or the prescribed trust management protocol execution.

Initially, all sensor nodes in the network are unselfish. A nodes selfish probability tends to be lower when a node has more energy and higher when the node has more unselfish neighbors as there are sufficient unselfish neighbors around to take care of sensor tasks.

3.3. Energy Model

Energy modeling is a key element in wireless network simulation. In several situations, the energy consumption at a particular node, or at a particular component of a node, is of interest. Further, energy consumed by a sensor node is an important metric for evaluating the performance of wireless network protocols. The energy model represents level of energy in a sensor node. The energy model in a node has an initial value which is the level of energy the node has at the beginning of the simulation which is known asinitial Energy of the sensor node i represented by E_{ij}^{init}. As the sensor node performs sensing, receiving and transmitting operations, energy is consumed by the sensor nodes. The residual energy of sensor node i represented by E_{ij}^{resi} decreases after every energy consuming operation. At any instant of time,

$$E_{ij}^{resi} <= E_{ij}^{init} \tag{11}$$

For each packet sent or received by a sensor node, a certain amount of energy is spent from the energy retained by the node. Furthermore, nodes idle energy consumption is specified. At every update interval, a procedure would be called to update the energy of every node on the network and comparison between the remaining energy and the threshold energy would be done to know whether the node is trustworthy or not. The same procedure would be repeated at every regular interval to update the energy of every node.

Cluster head initial energy E_{ch}^{init} and residual energy E_{ch}^{resi} are related by (12) which is similar

to normal sensor nodes.

$$E_{ch}^{resi} <= E_{ch}^{init} \quad (12)$$

The cluster head is given an initial energy higher than that of normal sensor nodes in the network because all the packets that have to reach the base station has to pass through the cluster head. So

$$E_{i}^{init} <= E_{ch}^{init} \quad (13)$$

for all cluster heads in the network.

4. IMPLEMENTATION

The proposed Trust-Based Hierarchical Routing protocol forms clusters with the available sensor nodes in the network. Then starting from the source node, the node which is closest to the destination with trust greater than the threshold value is chosen as the forwarding node. A cluster head or a cluster member node in the cluster can act as a forwarding node. Threshold trust is the value of trust below which, 100 % delivery of the packet to the destination node can be expected. In other words, the threshold trust is the marginal value of trust below which the node starts exhibiting malicious behavior. In the case of tie, the first node satisfying above criteria is utilized in forwarding the packet from source to the destination node. The process is repeated till the base station is reached.

The algorithm Trust-Based Hierarchical Routing is given in Table 1. The sensor nodes are provided with initial energy and initial trust. It is necessary to keep count of the trustable nodes in the network to find the lifetime of the network.

Data packets are generated for every sending period from source node to base station forming path through trustable nodes. After every transmission, the residual energy is updated for every sensor node participated in the transmission. The trust of every node is updated depending on its residual energy and communicating activities with its neighbors. For the next sending slot, the path from source to the base station is updated depending on the trust of the nodes. As the transmission continue, the number of trustable nodes in the network decreases. When this number falls below 35 % of total nodes in the network the possibility of a packet reaching the base station is very less. In order to maintain the packet delivery ratio, the packets are flooded, so that the packet reaches the base station, may be using a longer path. This introduces a large end-to-end delay in transmission, but packet delivery is ensured.

5. PERFORMANCE ANALYSIS

In this section, the numerical results obtained through network based evaluation are shown in the form of graphs. The simulator used in the implementation of routing protocol is NS2 [5], which is a widely used and accepted simulator for both wired and wireless networks. The parameters analyzed in this paper are network lifetime and packet delivery ratio of the network. Percentage of active nodes in the network as the simulation time proceeds is recorded for the trust based hierarchical routing and trust based geographical routing.

A wireless sensor network of 50 sensor nodes with 4 clusters evenly spread out in a 1000 m X 1000 m operational area is considered. The placement of nodes in the network is based on uniform distribution. The initial energy provided for sensor nodes is 2 J. Initially all the sensor nodes are assumed to have trust value of 1. As the network function continues the trust of nodes decreases depending on its interactions with its neighbors. Trust of all the sensor nodes in the network are updated at a regular interval of 0.2 seconds. Different network parameters and their values are summarized in Table 2. The sensor node becomes compromised when its trust falls less than 0.5. When the trust of a sensor node falls below 0.35 then it is not trustable and cannot take part in any of the network operations.

Trust Threshold is the value of the trust below which the sensor node cannot participate in transmission. Whenever trust of sensor a node

Table 1
Algorithm for Trust-Based Hierarchical Routing (TBHR) for Wireless Sensor Networks

Input: Wireless sensor network with sensor node positions.
Output: Chain of links from selected source sensor nodes to the sink node to transmit data packets.

1. For all sensor nodes assign initial energy.
2. For all sensor nodes assign trust as 1.
3. Form clusters of sensor nodes.
4. Assign count of trustable nodes as total number of nodes in the network.
5. Set simulation period.
6. Initiate transmission from selected sensor nodes towards the sink node.
7. For each packet transmitted update energy for transmission, reception and forwarding.
8. Update trust of participating nodes after each packet transmission.
9. Update packet count.
10. Update path from source to sink depending on the trust of nodes.
11. Update count of trustable nodes.
12. If number of trustable nodes is below 35 % of total nodes then flood the packet to reach sink node.
13. Repeat steps 6 13 for each data packet transmission till end of simulation time.

Table 2
Simulation Parameters and Values

Simulation Parameter	Value
Number of Nodes	50
Number of Clusters	4
Simulation Time	150 s
Traffic Generator	CBR
Monitoring Area	1000 X 1000 m^2
Communication Range	250 m
Packet Interval	0.2 s
Size of the Data Packet	500 bytes
Trust Range	[1,0]

falls below threshold value its neighbors with higher trust values will be used as forwarding nodes, allowing more sensor nodes to participate in transmission in the network. Thus the network is balanced and lifetime of the sensor network is increased. Figure 2 shows the graph of network lifetime when the trust threshold value is varied from 70 to 30 % of complete trust. Trust value of 1 repres ents complete trust, so, 70 % and 30 % of trust represents trust value of 0.7 and 0.3 respectively. The graph shows that there is an increase of around 10 % network lifetime in the case of Trust-Based Hierarchical Routing compared to that of Trust-Based Geographical Routing. The increase in network lifetime is because more number of nodes are participating in transmission and energy consumed by the network is near uniform in the network.

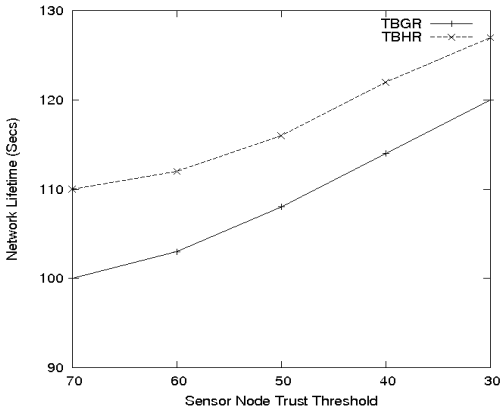

Figure 2. Sensor Node Trust Threshold versus Network Lifetime

Figure 3 shows the values of Packet Deliv-

ery Ratio of the rotocols Trust Based Hierarchical routing and AODV routing for number of compromised nodes in the network varying from 0 to 28. As the time proceeds the sensor nodes communicate with surrounding nodes and spend energy. This results in sensor nodes becoming compromised. As the number of compromised nodes increases the data packets are forwarded through trustable nodes to maintain the packet delivery ratio. For the proposed and implemented TBHR protocol when the number of compromised nodes crosses 24, which is nearly 50 % of total nodes, the packet delivery ratio drops. Flooding of packets is done in TBHR protocol at this stage, to maintain the packet delivery ratio of the network.

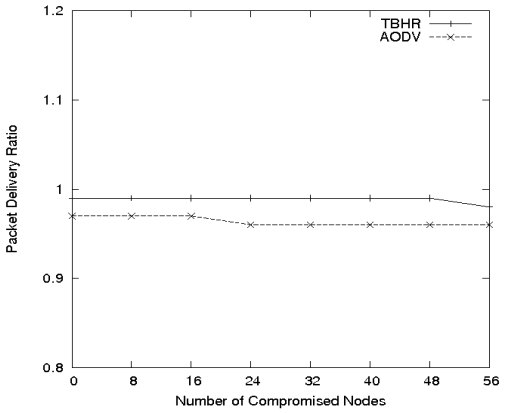

Figure 3. Number of Compromised Nodes in the Network Versus Delivery Ratio

The sensor nodes in the network that are not selfish, or compromised and are trustable, are active nodes of the network. Figure 4 shows the decrease in the percentage of active nodes in Trust-Based Hierarchical Routing and Trust-Based Geographical Routing protocols. The graph shows that for the first 40 seconds of simulation time, all the sensor nodes in the network are active. At 60 seconds TBHR protocol has all the nodes as active nodes, whereas for TBGR the same is reduced to less than 95 % of total nodes in the network.

The percentage of active nodes for TBHR protocol, is less than the same for TBGR protocol on an average of 4 % throughout simulation time. Sensor node trust value is initially one, and decreases as the network activities are carried out. The same is shown in Figure 5 for TBHR and TBGR protocols. Sensor node trust value at the end of simulation for TBHR protocol is 0.45, and for TBGR it is 0.25 that indicates the packet delivery factor at this time is very less. By using flooding technique, the packet delivery factor of the network is maintained at a higher value.

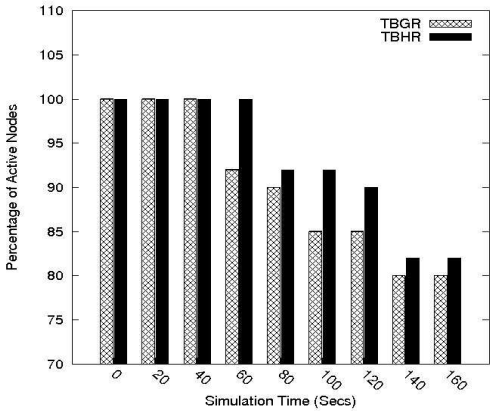

Figure 4. Simulation Time Versus Percentage of Active Nodes in the Network

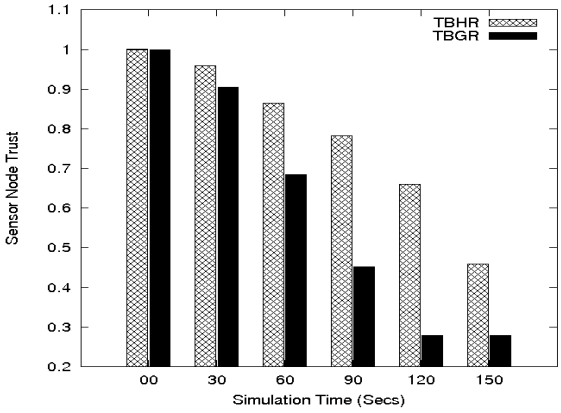

Figure 5. Simulation Time versus Sensor Node Trust

6. CONCLUSIONS

The role of different components of trust in routing information from source to destination in hierarchical wireless sensor network is discussed in this paper. The results indicated that Trust-Based Hierarchical Routing protocol performs around 10 % better than Trust-Based Geographical Routing with respect to network lifetime and nearly 5 % better than AODV protocol when the packet delivery ratio is considered. Throughout the simulation period the number of active nodes in Trust-Based Hierarchical Routing is more than or equal to the same in Trust-Based Geographical Routing. The flooding performed towards the end of simulation introduces additional end-to-end delay in packet transmission. One of the future directions in this research work is to reduce the end-to-end delay in packet transmission in the network.

REFERENCES

1. H Karl and A Willig. Protocols and Architectures for Wireless Sensor Networks, *Germany: John Wiley and Sons*, 2005.
2. X Y Ali. Wireless Ad Hoc and Sensor Networks, Illinois Institute of Technology, *Cambridge University Press*, 2008
3. W Heinzelman, A Chandrakasan and H Balakrishnan. Energy Efficient Communication Protocol for Wireless Microsensor Networks, *in Proceedings of the* $33^{r}d$ *Annual Hawaii International Conference on System Sciences,* 2, Jan 2000.
4. Fenye Bao, Ing-Ray Chen, Moon Jeong Chang and Jin-Hee Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, *IEEE Transactions On Network and Service Management,* 9(2):169–184, June 2012.
5. Eitan Altman and Tania Gimenez. *NS Simulator for Beginners, Lecture Notes,* 2003.
6. Junqi Duan, Dong Yang, Haoqing Zhu, Sidong Zhang and Jing Zhao. TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks, *International Journal of Distributed Sensor Networks,* Article ID 209436, pages 1-14, 2014.
7. E Aivaloglou and S Gritzalis. Hybrid Trust and Reputation Management for Sensor Networks, *Wireless Networks,* 16(5):1493–1510, July 2010.
8. K Liu, N Abu-ghazaleh, and K D Kang. Location Verification and Trust Management for Resilient Geographic Routing, *Journal on Parallel Distribution and Computing,* 67(2):215–228, February 2007.
9. Riaz Ahmed Shaikh,Hassan Jameel,Brian J d'Auriol,Heejo Lee,Sungyoung Lee andYoung Jae Song. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems,*DOI 20:1698-1712. DOI:10.1109/TPDS.2008.258, 2009.
10. Zhang G, Zhang Y, Chen Z. Using Trust to Secure Geographic and Energy Aware Routing against Multiple Attacks, *PLoS ONE,* 8(10), e77488. doi: 10.1371/journal.pone.0077488, 2013.
11. Ajith Kumar S, Knut vsthus and Lars M Kristensen. An Industrial Perspective on Wireless Sensor Networks - A Survey of Requirements, Protocols and Challenges, *IEEE Communications Surveys and Tutorials,* 16(3), January 2014.
12. M A Simplcio Jr, P S L M Barreto, C B Margia and T C M B Carvalho. A Survey on Key Management Mechanisms for Distributed Wireless Sensor Networks, *Computer Networks,* 54(15), pages 2591-2612, October 2010.
13. Mohammad Momani and Subhash Challa. Survey of Trust Models in Different Network Domains, CoRR, DOI: abs/1010.0168, 2010.
14. Junqi Zhang,Rajan Shankaran,Mehmet A Orgun,Vijay Varadharajan andAbdul Sattar. A Trust Management Architecture for Hierarchical Wireless Sensor Networks, pages 264-267, DOI:10.1109/LCN.2010. 5735718, 2010.
15. Hui Xia, Zhiping Jia, Lei Ju1, Xin Li and Youqin Zhu. A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules, *IEEE/ACM International Conference on Green Computing and Communications,* pages 124–130, 2011.
16. J H Cho, A Swami and I R Chen. A Survey on Trust Management for Mobile Ad hoc Networks, *IEEE Communication Surveys Tutorials,* 13(4):562–583, 2011.
17. D A Tran and H Raghavendra. Congestion Adaptive Routing in Mobile Ad-hoc Networks, *IEEE Transactions on Parallel and Distributed*

Systems, 17(11):1294–1305, 2006.
18. D D Couto, D Aguayo, J Bicket and R Morris. A High-Throughput Path Metric for Multi-Hop Wireless Routing, *In Proceedings of ACM International Conference on Mobile Computer Networks,* pages 134–146, september 2003.
19. E Aivaloglou and S Gritzalis. Hybrid Trust and Reputation Management for Sensor Networks, *Wireless Networks,* 16(5):1493–1510, July 2010.
20. Liu, N Abu-ghazaleh and K D Kang. Location Verification and Trust Management for Resilient Geographic Routing, *Journal of Parallel Distributed Computing,* 67(2):215–228, February 2007.

Yamuna Devi C R is currently pursuing Ph.D in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. She obtained her Bachelor of Engineering degree in computer Science and Engineering branch. Her research interest is in the area of Wireless Sensor Networks.

Saishiva K is a BE Graduate in Computer Science and Engineering branch from University Visvesvaraya College of Engineering, Bangalore University, Bangalore.

Sunil Kumar is a BE Graduate in Computer Science and Engineering branch from University Visvesvaraya College of Engineering, Bangalore University, Bangalore.

S H Manjula is currently working as Associate Professor, in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. She obtained her Bachelor of Engineering, Masters of Engineering and Ph.D in Computer Science and Engineering. She has published a book on Wireless Sensor Networks. She has published more than 45 papers in refereed international journals and conferences. Her research interests are in the field of Wireless Sensor Networks, Semantic web and Datamining.

Venugopal K R is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras.He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 51 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems *etc.*, He has filed 53 patents. During his three decades of service at UVCE he has over 400 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is currently Honorary Professor, Indian Institute of Science, Bangalore, India. He was a Vice Chancellor, Defense Institute of Advanced Technology, Pune, India and was a Professor since 1986 with the Department of CSA, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD, Soft Computing and Computational Neuroscience.