Trustworthy Route formation Algorithm for WSNs

Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar
Department of Electronics and Telecommunication Engineering
Jadavpur University, Kolkata – 700 032
West Bengal, India

ABSTRACT
This paper introduces a new algorithm for the formation of trustworthy route from source node to Base Station (BS) for secure routing of messages in Wireless Sensor Networks (WSNs). This algorithm process the information given by the Trust dependent Link State Routing Protocol which is improved version of our Routing Protocol presented in [1] Direct Trust dependent Link State Routing Protocol based on Geometric Mean (GM) of the QoS characteristics which allows the trusted nodes only to participate in the routing. Execution of this algorithm at any node, gives different trusted routes to the BS with different route trusts by filtering the un-trusted nodes on the basis of trust metrics levels. The source node selects the best trustworthy route among many trusted routes given by the neighbor nodes based on neighbor nodes trust levels and the route trust levels of different routes given by them. The newly formed trustworthy route from source node to BS will be the best trustworthy route without considering the malicious/selfish nodes.

Keywords

Wireless Sensor Network (WSN), Geometric Mean (GM), Trust Metrics, Base Station (BS).

1. INTRODUCTION
Wireless Sensor Networks offer solutions which covers wide range of applications. Depending on the application, their deployment environment may be hazardous, unattended and some times dangerous. The Cryptographic Security Systems in WSNs can not detect the node physical capture, the malicious or selfish nodes. Hence, new security systems are required for secure routing of message from source to BS (sink) of WSNs. A new way of getting security without using cryptography is Trust based security in WSNs. Trust [2] is "The degree of Reliability" of other node in performing actions and can be formed by maintaining a record of the transactions with other nodes directly as well as indirectly. From this record a trust value will be established. Trust management system for WSNs, is a mechanism that can be used to support the decision-making processes of the network [2]. It aids the members of WSN (trustors) to deal with uncertainty about the future actions of other participants (trustees).

Many researches on trust related in WSN are processed, but it is required to design and develop a light weight trust management system that takes the less resources of the node in evaluation and management of trust between/among the nodes. The trust management of the WSN should be as simple as possible, i.e. without constraints on energy consumption, software, hardware, memory usage, computing, processing speed and communication bandwidth, and it should detect the different attacks easily, and mange and update trust relations accordingly.

In this paper, we extend our previous work presented in [1] Direct Trust dependent Link State Routing Protocol (DTLSRP), that finds the Trustworthy Route based on Direct Trust only. Both Direct Trust and Indirect Trust are taken into account to form final Trust on a node and Trustworthy Route from source ti sink. A new algorithm is developed for selecting the Trustworthy Route from source node to the Base Station for secure routing of messages. This algorithm, process the output information given by Trust dependent LSR Protocol which allows the trusted nodes only to participate in routing messages.

The rest of this paper is organized as follows: first in section 2 we present the related work on Trust based Routing models in WSN and in section 3 the trust dependent routing protocol among the benevolent nodes and the Trustworthy Route from source to sink (BS) formation algorithm and section 4 simulation, section 5 conclusion and future scope of the paper.

2. TRUST BASED ROUTING METHODS
Enhancements in the routing related protocols based on the trust have been widely addressed in the literature. The following are the most important research results in this direction:

ARIADNE: It is very efficient protocol, using highly efficient symmetric cryptographic primitives and per-hop hashing function [3]. It prevents the attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks.

ATSR (Ambient Trust Sensor Routing): A fully distributed Trust Management System is realized in ATSR [4] in order to evaluate the reliability of the nodes. Using this approach, nodes monitor the behavior of their neighbors in respect to different trust metrics and finds direct trust value per neighbor.

Trusted AODV: It is an extended AODV routing protocol to perform routing by taking trust metrics into account [5]. First, a trust recommendation mechanism introduced and then the routing decision rules of AODV are modified to take trust into account.

Trusted GPSR: The Greedy Perimeter Stateless Routing [6] is modified to take trust levels of node into account. Each time a node sends out a packet it waits until it overhears its neighboring node forwarding it. Based on this correct and prompt forwarding information it maintains a trust value for its neighbors. This information is then taken into account in the routing decisions.

SPINS: This [7] has been designed to provide data authentication, data confidentiality and evidence of data freshness. In this protocol two security blocks SNEP and µTESLA are involved. The first block introduces overhead of 8 bytes and maintains a counter fro achieving semantic security. µTESLA provides authentication for data broadcasting. Though SPINS claim to provide trusted routing ensuring data authentication and confidentiality, but it does not deal with Denial of Service Attacks.

Trust- aware DSR: The watchdog and Pathrater modules has been designed and incorporated in the Dynamic Source Routing protocol for security [8]. The watchdog module is responsible for detecting selfish nodes that do not forward packets. For this, each node in the network buffers every transmitted packet for a limited period. During this period each node enters into promiscuous mode in order to overhear whether the next node has forwarded the packet or not.

CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks): This [9] protocol adds reputation system and a trust manager to the Watchdog and Pathrater scheme. The trust manager evaluates the events reported by the Watchdog and issues signals to other nodes regarding malicious nodes. The signal recipients are maintained in a friends-list. The reputation system maintains a black-list of nodes at each node and shares them with friends-list nodes.

TRANS: TRANS [10] routing protocol selects routes based on trust information not on hop count to avoid the insecure locations. This protocol assumes that the sensors know their locations and that geographic routing is used. A sink sends a message only to its trusted neighbors for the destined location. Those corresponding neighbors forward the packet to their trusted neighbors that have the nearest location to destination. Thus the packet reaches the destination along a path of trusted sensors.

3. TRUST DEPENDENT LINK STATE ROUTING PROTOCOL (TLSRP)

Mohammad Momani [2] introduced a computational model for trust in his doctorate thesis. He modelled the direct trust computation with direct experiences, and indirect trust with recommendations given by the neighbors. The direct trust **A** of node N_1 on node N_2 is defined as the sum of trust values node N_1 is having on node N_2 for different trust metrics (using traditional weighting approach of the QoS characteristics). The indirect trust **B** of node N_1 on node N_2 is defined as the average of recommendations given by the neighbors of node N_2 (nodes N_3, N_4, N_5, N_6 and N_7) as shown in Fig. 1. He modelled total trust C using traditional weighting approach for direct trust and indirect trust as shown in following Equation 1.

$$\mathbf{C = A * W_A + B * W_B} \quad (1)$$

Node N_1 (Blue color) wants to find the trust on N_2 (Red color).
Node N_2 neighbor nodes are N_3,,N_4, N_5, N_6 and N_7.

- Dashed arrow indicates the Indirect information about node N_2 given by its neighbors to node N_1.
- Solid arrow indicates the Direct Experience.

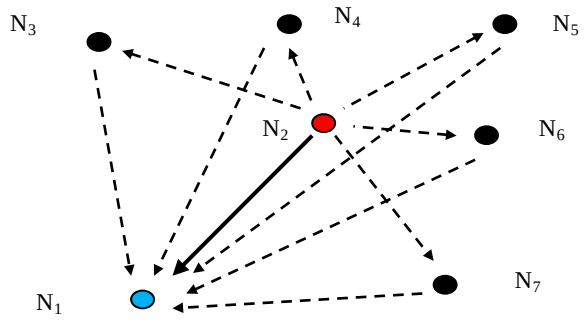

Fig. 1. Node's trust relationship.

The weights W_A and W_B can be assigned using different approaches. Some nodes may be given more weight for direct trust; others may be given more weight in indirect trust. i.e. $W_A > W_B$ or $W_A < W_B$. Weights to the direct trusts of some metrics may be given more importance, and others are less importance. Similarly, for indirect trusts nearby nodes may be given more importance and others is less importance.

We proposed new routing protocol [1] suitable for many practical applications of the Wireless Sensor Networks (WSNs). The Trust Management System (TMS) is a part of the proposed routing protocol. The Trust of any node is evaluated based on the geometric mean of trust metrics of the node (direct trust), and geometric mean of information given by the node's surrounding (neighbor) nodes. The node's information given by neighbor nodes (indirect trust) is nothing but, their direct trusts with the node. Every node in the network, will maintain a database record for every its neighbor node. This record contains the information about different trust metrics, i.e. QoS characteristics for all its neighbors regarding the number of events occurred in the network. This trust metrics data will be helpful for calculating the direct trust of its every neighbor node. Also, as and when required, trust metric data of one node, can be transferred to other nodes, where it acts as information (indirect) in calculating indirect trust of the node.

The proposed trust model is a decentralized trust scheme, i.e. the trust management functionality is distributed over the network nodes. Each node is responsible for computing its own trust value per relation in the network, collecting events from direct relations, and collecting trust values from other nodes in the network (in other words, indirect information). This means that both direct and indirect trust values are used to evaluate each node's trustworthiness. The indirect (second-hand) information may be particularly useful when no node is showing trustworthiness with direct interaction, i.e. when the situation is

risky, then indirect trust plays major role in the formation of trust on any node.

One of the most important functions of trust management schemes is the process of data collection for trust evaluation. The direct trust value of a neighboring node can be determined by the different trust metrics of that particular node in different events occurred in the network. The trust metrics, i.e. the QoS characteristics that can be taken into account are Data packets forwarded, Control packet/ message forwarded, Availability based on beacon/hello messages, Routing protocol execution (routing actions), Consistency of reported (sensed) values/data, Sensing communication, Reputation and Energy level etc.

The trust metrics data for different events are essential and can provide a useful feedback to the system, towards the proper decision making by the trust management system. Here, depending on the application, we can insist the minimum level (threshold) to all the trust metrics, or we can have different thresholds to different groups of trust metrics. Once one/more trust metric threshold/s are fixed, our trust management system see that no node is trusted unless the node is having minimum threshold level in a given trust metric strictly. This is the main advantage of our proposed trust management model comparing with other models.

In this trust management system, the direct trust is Geometric Mean of all different trust metrics for different events occurred in the network on that particular node. These trust metrics are different from the trust metrics of other surrounding nodes. Like this, every node will be having a separate record of data of every surrounding node in different trust metrics for different events occurred in the network. From these records, Direct Trust (DT) is calculated based on Geometric Mean of the QoS characteristics as given in the below Equations 2 and 3.

$$\mathbf{DT = [\ \prod(m_1, m_2, m_3, ..., m_{10})\ ]^{(1/10)}} \quad (2)$$

$$\mathbf{DT_I(J) = [\ \prod_K(\ m_{I,J,K})\ ]^{1/K}} \quad (3)$$

In Equation 2, m_1, m_2, m_3, ... , m_{10} are the ten different trust metrics (assumed) of node. In Equation 3, the DT_I (J) is the Direct Trust value of node I on node J, calculated for K different type of trust metrics. Every node maintains the database of all its neighbors, and the contents of database are direct trust, indirect trust, different trust metrics and trust evaluation, etc.

The Indirect Trust (IT) on node N_2 with respect to N_1 can be calculated from the direct trusts (DTs on N_2 with respect to its neighbors) sent by the neighboring nodes of N_2. The Indirect Trust of node N_1 on node N_2 is defined as the Geometric Mean of the DTs of neighbor nodes (N_3, N_4, N_5, N_6, and N7 as per Fig 1.) on N_2. This is shown in Equations 4 and 5.

$$\mathbf{IT = [\ \prod(DT_1, DT_2, DT_3, ..., DT_8)\ ]^{(1/8)}} \quad (4)$$

$$\mathbf{IT_I(J) = \{\ \prod_L [DT_L(J)]\ \}^{1/L}} \quad (5)$$

Here, DT_1, DT_2, ..., DT_8 are the DTs given by the neighbor nodes. The IT_I (J) is the Indirect Trust value of node I on node J, calculated for indirectly given information by L neighbors of J. The Equation 4 gives IT of node assuming 8 neighbors. The Equation 5 is generalized for the calculation of IT of node I on node J based on information given by L neighbors. These neighbors supply their Direct Trusts on node J which will be helpful for finding Indirect Trust at node I on node J. The total trust of any node with respect to any other node is again a function of Direct Trust (DT) and Indirect Trust (IT). Our proposed model also uses the traditional weighting approach as in [2] for combining Direct Trust (DT) and Indirect Trust (IT) and form the total Trust (T) per relation in the network as shown in Equation 6.

$$\mathbf{T = W_D * DT + W_I * IT} \quad (6)$$

The weights W_D is weightage given to DT and W_I to the IT where $W_D + W_I = 1$. Weights can be assigned using different approaches. Depending on the application, some times DT may be given more weight, and IT may be given less weight i.e. $W_D > W_I$, and vice-versa.

3.1 Trustworthy Route selection Algorithm:

Every node in the WSN, finds the trustworthiness with its neighbor nodes based on the said geometric mean based Trust Evaluation method. Every node maintains the database of different trust metric parameters of its neighbors. Similarly, every node (except Base Station) runs the Trust dependent LSR Protocol (it doesn't require to run Dijsktra's algorithm or any other algorithm to find the shortest path from node to sink because, highest *route trust* route automatically evaluates shortest path), and finds the best Route to the Base Station. Depending on the application, this will be done periodically by the all nodes to maintain different routes with different route trusts. The source node, i.e. the node which has the packet/message of data to be transmitted to the Base Station, also runs the Trust dependent LSR Protocol and gets the Trustworthy Routes given by its neighbor nodes. Then the source node selects one best Trustworthy Route among many, depending on the neighbor nodes Trust (Ts) and the Route Trusts (RTs) given by them using the following algorithm.

All the nodes in WSN should run the following algorithm (from step 1 to step 3) periodically for finding Trusts for their neighbor nodes and evaluate the trusted routes to the sink node. The step 4 should run by the nodes those are participating in the trustworthy routing (i.e. all the nodes of the trustworthy route starting from source node except sink node).

ALGORITHM:

Step 1:

{

- Get the all trust metrics data of all neighbor nodes.
- Evaluate Direct Trusts (DTs) of node on all neighbor nodes as per Equation 3.

- Get the Direct Trusts (DTs) of all neighbor nodes on their neighbor nodes.
- Evaluate Indirect Trusts (IT) of node on all neighbor nodes as per Equation 5.
- Evaluate the Trusts (Ts) of the node on all neighbor nodes.
- Make entry in the Table 1. that contains Trust (T) values of neighbor nodes.
- Based on Trust Threshold (T_{th}), find and mark the benevolent nodes in Table 1.

}

Step 2:

- Run the Link State Routing Protocol (LSRP) with the benevolent nodes found in Table 1, and gets the information from other benevolent nodes about different Trusted Routes to the sink, with their Route Trusts.
- Make entry in the Table 2. with this information.

Step 3:

- Compare Table 1. with Table 2. and Evaluate multiplicative Route Trust (RT x T) and select the best Route (R) and neighbor node (N) whose Route Trust (RT) is greater than Trust Threshold (T_{th}) level.

Step 4:

- Using the best Trustworthy transmit the data/message to the sink.
- The trust metrics of neighbors those are found benevolent and present in the Selected Route should be hiked (say +0.001).
- Similarly, the trust metrics of all other neighbor nodes those found benevolent but, are not participating in selected Route should also be increased (say +0.0005).
- Similarly, all other neighbor nodes those are not found as benevolent nodes should be penalized and their respective trust metric should be decreased (say -0.001).

End.

Table 1. Neighbor node Trusts

Neighbor node	Trust
N_1	T_1
N_2	T_2
N_3	T_3
N_4	T_4
N_5	T_5
N_6	T_6
..	..

Table 2. DTLSRP information from neighbors nodes

Neighbor node	Routes to BS	Route Trust
N_1	R_1	RT_1
N_1	R_2	RT_2
N_2	R_3	RT_3
N_2	R_4	RT_4
N_3	R_5	RT_5
N_3	R_6	RT_6
..	..	..

4. SIMULATION

Place In the proposed algorithm, there are two parts. One is trust evaluation system, and the other is trustworthy routing with the benevolent nodes of the WSN. The performance evaluation of the first part has been done through computer simulations. A new software simulation package has been developed using the MATLAB platform to evaluate the trust of the node with respect to other node. To form the trusted relation between two adjacent nodes (say I and J as shown in Fig. 2.), the Trust Evaluation (TE) level is formed and is given by the average of trusts of each other as shown in Equations 7. Here, $T_i(J)$ is trust of node I on node J, and $T_j(I)$ is trust of node J on node I. This is because, Trustworthy relation formation between two nodes means, both the nodes should trust upon each other.

$$\mathbf{TE_{I,J} \text{ or } TE_{J,I} = [T_I(J) + T_J(I)]/2} \quad (7)$$

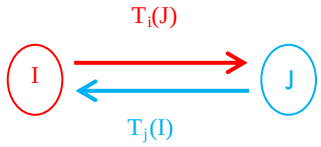

Fig. 2. Trust Evaluation between two nodes.

The Fig 3. shows the graphical result of simulations for trustworthy relations formed among the benevolent nodes of WSN. The parameters used are, 6 X 6 node WSN, 8 neighbor nodes, 10 different trust metrics taken randomly between 0 and 1. And Direct Trust (DT) threshold = 0.6, and Indirect Trust (IT) threshold = 0.4.

The second part of our proposed model is Trustworthy Route formation algorithm. By applying our Trust dependent LSRP algorithm, we can form the best Trustworthy Route from source node to sink (BS).

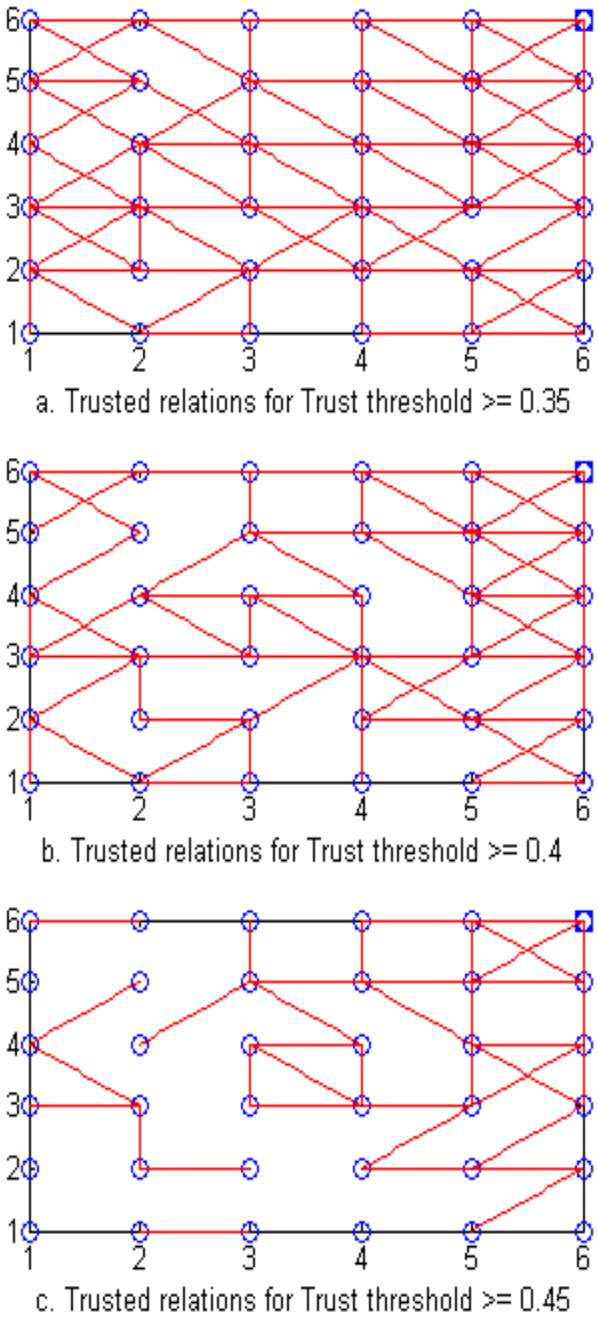

Fig. 3. Trustworthy Relations for different T_{th}

5. CONCLUSION AND FUTURE SCOPE

In this paper we presented a new algorithm for the formation of Trustworthy Route from source node to sink for WSN using the Trust (both Direct and Indirect) dependent Link State Routing Protocol. Trust is calculated based on geometric mean of QoS characteristics of the node and the experiences offered by the neighbors of the node. The proposed model is simple and is modified LSR Protocol. At this stage, the first part of the algorithm, i.e. formation of trusted paths between benevolent nodes is simulated. And we are in the process of the second part simulation, i.e. Trustworthy Route formation from any node (source) to sink. In the future we extend this algorithm to application specific adaptive trust algorithm basing on the risk, in which the trust management at any node shall be so simple, i.e. without constraints on energy consumption, software, hardware, memory usage, computing, processing speed and communication bandwidth. We shall also develop a new algorithms to detect the different attacks easily, mange trust relations accordingly and it shall also be able to manage other dynamic aspect of trust i.e. trust revocation.

6. REFERENCES

[1] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar, "A Direct Trust Dependent Link State Routing Protocol Using Route Trusts for WSNs (DTLSRP)", Scientific Research, an international journal on Wireless Sensor Network, 2011, 3, 125-134. doi:10.4236/wsn.2011.34015.

[2] M. Momani, "Bayesian Methods for Modeling and Management of Trust in Wireless Sensor Networks," Ph.D. Thesis, University of Technology, Sydney, July, 2008.

[3] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. Eighth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom), pp. 12-23.

[4] Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis, "Mobile Networks Trust Management in Wireless Sensor Networks", *European Transactions on Telecommunications*, 2010; 21:386-395.

[5] Xiaoqi Li, Lyu, M.R., Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad-hoc Networks", IEEE Proceedings on Aerospace Conference, 2004, vol. 2.

[6] Asad Amir Pirzada and Chris McDonald, "Trusted Greedy Perimeter Stateless Routing", IEEE, ICON 2007.

[7] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, "SPINS: Security Protocols for Sensor Networks", ACM Journal of Wireless Networks, 8:5, September 2002, pp. 521 – 534.

[8] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), ACM Press, 2000, pp. 255 – 265.

[9] S. Buchegger and J. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Ad-hoc Networks", in proceedings of the 3rd ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc), ACM Press, 2002, pp. 226-236.

[10] Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy, "Location-centric Isolation of Misbehavior and Trust routing in Energy-constrained Sensor Networks", IEEE International Conference on Performance, Computing and communications, 2004.