Collaborative Approach for Secure Packet Transfer in Wireless Sensor Networks

Yenumula B. Reddy and Sanjeeve Kafley
Grambling State University
Grambling, LA 71245, USA
ybreddy@gram.edu

Rastko Selmic
Louisiana Tech University
Ruston, LA 71270, USA
rselmic@latech.edu

***Abstract*- Secure data transfer (SDT) in wireless networks is required with minimum overhead. The SDT was done historically through cryptography, authentication, and probability based approaches. Collaborative approach for trust-based packet transfer is new to the wireless sensor network research. In the proposed research, trust value of a node is continuously updated using Sporas formula and repeated trust calculations. The average of these two provides the trust value of a node. The suspicious node will be informed to the neighbor nodes. Further, the neighbor nodes calculate their own trust of a suspicious node using its trust value plus trust factor received from their neighbor. The cooperative and collaborative approaches eliminate the suspicious node from the path quickly and confidently. The results show that the new approach is better than simply using the cooperative way or collaborative approach using Sporas formula.**

Keywords: packet transfer, wireless sensor networks, collaborative approach, protocols, trust-based approach, resource.

1. INTRODUCTION

Massive deployment of sensors in hostile areas including forests, biological and chemical fields is very common and requires secure communication. Replacement of failing sensors or adding sensors to cover the black holes is very common in such dangerous places. Since they are organized in an open environment, injecting of bad nodes to corrupt the transmission is possible. Therefore, a secure transmission model is required to avoid the transmission through corrupted node. Further, design of secure communication model between sensor nodes is very difficult. The traditional protocols use exchange and distribute the keys through cryptographic tools for trust evidence. The resource limitations in sensor networks obstruct the use of traditional tools including cryptographic models and protocols for secure communications.

In sensor networks, the topology changes dynamically due to failure of sensors nodes. Further, sensing data and reporting data with limited communication distance requires cooperation of nodes to complete the task. The cooperation happens between the nodes only if they trust their neighbor to transfer the data. The trust management system helps to detect the node that is not behaving as expected in the path.

The trust depends upon the predictable behavior of other nodes in the network and builds upon continuous positive behavior. Further, trust depends upon the degree of belief based upon the experience. Trust is subjective, non-transferable, time dependent, contextual, and unidirectional. Due to the simplicity and effectiveness of the trust and reputation based models researchers' attention is diverted towards these models.

The trust starts with sensing the behavior of the neighbor node. The misbehavior is dropping the packets. The packet dropping may be due to malicious attacks (influence of bad nodes or intruders) on the node or the node is a sink hole. The trust can be measured through repeated positive behavior of the node. Reputation is a tool to detect the good behavior of the neighboring node [1]. The node could be assigned a reputation value to detect the behavior and keep track of the next node (forward path) in the path. To prove the successive node in the path is trustworthy, the current node should maintain a table. The table must contain the number of packets received and transmitted from the successive node. Further, it matches the table by overhearing from the next node, which transmits the packets to its neighbor. All nodes in the path will follow this process. The table includes the number of transmitted packets and will be initialized to zero after a set time. The method is simple with minimum resource utilization and easy to maintain. The design of such simple and low cost secure model is very important and an open research area.

Routing the packets in wireless sensor networks (WSN) is done by routing protocols. The routing procedure uses encryption, digital signature, and authentication. Further encryption and authentication limits the performance of nodes in WSNs. Encryption and authentication cannot prevent the malicious or misbehavior of the sensor nodes. After reviewing relevant sensor network models, we found that the trust-based model is a better model than the existing models. Since trust cannot be generated automatically, we use the verification of repeated data transfer in the successive node. The trust model detects the sinkholes, selective packet dropping, and malfunction of the node.

Once the trust is established, it cannot be taken for granted for the rest of the sensor lifetime without repeated reevaluations. The trust relationship changes continuously due to sensor failures and malfunctions. Therefore, the

Copyright (c) IARIA, 2011. ISBN: 978-1-61208-144-1

trust relationships among the neighboring nodes are very important to keep track of the uncertainties.

The remaining part of the paper discusses the recent developments, collaborative reputation activity, simulations using Sporas formula, reputation-based trust formulation, trust cluster approach and conclusion of results.

2. Recent Developments

If a user is given the work repeatedly and the user completes to the level of satisfaction, we say the user will be trusted. The same concept is used in credit cards, bank loans, and at work places. Sensor networks are not different when we consider the trust. The Figure 1 shows the scenario of a senor network. The nodes A, B, C are transferring the data to their successive node D, where D transfers to its next successive node E. The level of trust of a node D depends upon the percentage of packets successfully transferred to its next successive node E. The trust of node D depends upon the behavior of node D at a given time. The trust evaluation of node D also monitored through the neighboring nodes (node B and node C within communication distance) of A.

Trust values are derived in [2] by evaluating risk and reputation. In [3] the authors developed an algorithm to calculate trust using the complaints of another agent. Reputation-based framework using Bayesian formulation was developed by Generiwal et al. [4]. The proposed system uses community trustworthy behavior of the sensor nodes. The trust calculation in WSN using a bio-inspired algorithm (BTRM-WSN) based on ant colony systems was presented in [5]. The system uses similarity of how the ants' deposited pheromone helps to trace the path and quality of path by trusting the deposited pheromone.

Momani et Al. [6], explained the difference between trust, security, and reputation. Further, authors introduced the WSN security issues and innovative approaches to solve these problems. The authors concluded that the future research follows the innovative approach to model trust-based approach in WSN.

Task-based trust management, event-based trust management and an agent-based trust management was studied in [7-11]. In [7], a general approach for task-based trust management is used similar to economics to detect the malicious node. The event-based approach [8] uses several trust ratings to enforce the security in WSN. The agent-based trust models in [8-11] discuss the attacks on WSN, packet dropping, and local storage management using the trust policy. The models can further discusses the trust aggregation, Hello flood attack, and detect the malicious nodes.

Zhang et al. [12] presented a trust-based approach to distinguish illegal nodes from legal nodes. They claim that their approach detects insider attacks and uses trust evaluation model. The trust management model in [13] uses the Bayesian probabilistic approach. The current model calculates the trust factor by using the current trust factor plus the second hand information received from its neighboring nodes.

3. Collaborative Reputation activity

Reputation builds the trust in a specific domain. Reputation-based trust was discussed in [14] and defined as the amount of trust influenced by a person or node in a specific domain. Like with human relationships, reputation values associated with a node may change over a time. Therefore, it is advised to update the node ratings using current ratings. This procedure helps to calculate better trust factor. The reason for changing the trust rates overtime is that the node may get corrupt due to malicious activity.

Assume that each node entering in the sensor network has a minimum reputation value, i.e., initially every node transfers packets correctly. The node value will be updated after a set time period. A threshold value (trust value) will be set to decide either the node will continue in the communication path or discord at the end of each set period. In a sensor network, a new node can join the existing set of sensors or a malicious sensor will be discarded from communicating path (Similar to an electronic market, a new user may join in the group or untrusted member may discontinue). The reputation value of a current node should not fall below the newly joined node. A node can rate the neighboring node more than once, but the current rating will be taken. A higher rated node will have smaller change after each rating (unless the node is corrupted).

The sample rating of a neighboring node is done depending upon the trust. Trust of each node depends upon the opinion of other nodes, particularly neighboring nodes. Trust of a node is continuous updating through rating. The current reputation of a node (trust level) is updated using the following Sporas formula [15].

$$R_i = R_{i-1} + \frac{1}{\theta}.\phi(R_{i-1}).(W_i - R_{i-1}) \qquad (1)$$

$$\phi(R_{i-1}) = 1 - \frac{1}{1 + e^{-(R_{i-1}-D)/\sigma}} \qquad (2)$$

where:

θ - effective number of ratings taken into account $(\theta > 1)$. The change in rating should not be very large.

ϕ - helps to slow down the incremental change

W_i - represents the rating given by the node i

D - range or maximum reputation value

σ - the acceleration factor to keep the ϕ above certain value (> threshold).

If the node is compromised, the rating will be smaller and $(W_i - R_{i-1})$ become negative. Therefore the current

Copyright (c) IARIA, 2011.
ISBN: 978-1-61208-144-1

reputation slowly crosses below threshold and node declared as malicious.

In the Figure 1, the opinion poll on node D will be done by nodes A, B, C, and P, because these nodes communicates the packets through D to the base station. The node E cannot poll on D, since it receives the packets from D. Assume that there is a node Z between E and base station, then E can poll on D, because if Z becomes malicious then E may need to transfer the data through D to reach the base station. In the opinion poll, the node A may poll 70% and node B may poll 80%. Sporas formula updates the rating (helps to build the trust) on node D using the rates polled by the connected nodes.

4. Simulations Using Sporas Formula

Suppose the node A makes 50 transactions and each time the node A give its own rating depends upon the number of packets transmits by the node D. Figure 2 provides the ratings on node D obtained by node A. Similarly, the ratings at B and C were found. The random values selected to calculate the ratings are as below:

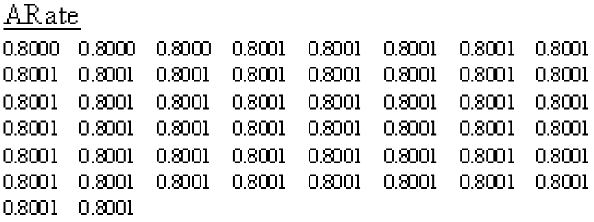
θ>10; 0.5<W_i<1;

0.6<D<0.99 0<σ<0.5;

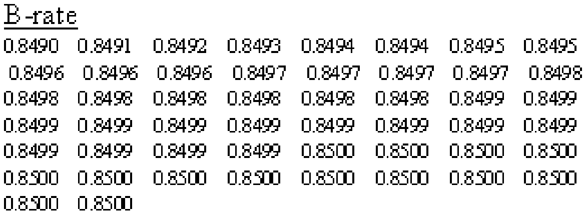
0.5<R_{i-1}<1;

Table I provides the ratings after 50 samples. Each time the rate was updated with the current value. At 50th time (current ratings at A, B, and C are 0.8001, 0.85, and 0.90. Suppose the threshold value is set at 0.85, then the node A requests the neighbor nodes C and D about the trust of node D. The nodes B and C give their trust value 0.85 and 0.9. The node A cannot discard the node D from its communication path, but it uses the reputation based trust calculation as given in the next section and will come to a conclusion.

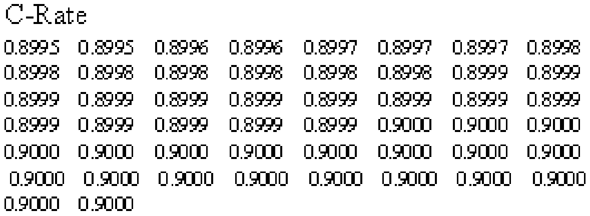
Table I: Ratings of node D at Nodes A, B, and C



```
ARate
0.8000  0.8000  0.8000  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001  0.8001
0.8001  0.8001
```



```
B-rate
0.8490  0.8491  0.8492  0.8493  0.8494  0.8494  0.8495  0.8495
 0.8496  0.8496  0.8496  0.8497  0.8497  0.8497  0.8497  0.8498
0.8498  0.8498  0.8498  0.8498  0.8498  0.8498  0.8499  0.8499
0.8499  0.8499  0.8499  0.8499  0.8499  0.8499  0.8499  0.8499
0.8499  0.8499  0.8499  0.8499  0.8500  0.8500  0.8500  0.8500
0.8500  0.8500  0.8500  0.8500  0.8500  0.8500  0.8500  0.8500
0.8500  0.8500
```



```
C-Rate
0.8995  0.8995  0.8996  0.8996  0.8997  0.8997  0.8997  0.8998
0.8998  0.8998  0.8998  0.8998  0.8998  0.8998  0.8999  0.8999
0.8999  0.8999  0.8999  0.8999  0.8999  0.8999  0.8999  0.8999
0.8999  0.8999  0.8999  0.8999  0.8999  0.9000  0.9000  0.9000
0.9000  0.9000  0.9000  0.9000  0.9000  0.9000  0.9000  0.9000
 0.9000  0.9000  0.9000  0.9000  0.9000  0.9000  0.9000  0.9000
0.9000  0.9000
```

5. Reputation-based Trust Formulation

The Sporas formula updates the node reputation to current status. The reputation status value of each node is stored by its neighboring nodes. Therefore, each node maintains a table and stores the reputation status of its neighboring node or nodes. If any node gets malicious, then the connected nodes change the reputation value in their table. If the value of a node drops below the threshold, then the node will be declared as malicious. The declared malicious node will be disconnected from the network.

The reputation of a node is calculated average of two methods. First, reputation value is calculated through Sporas formula using equation (1) basing on opinion poll. Second, reputation of a neighboring node is calculated using the ratio of the number of packets sent to the node (S_m) to the number of packets forwarded (F_n) by the node.

$$R_{nm} = \frac{F_n}{S_m} \tag{3}$$

The ratio $F_n / S_m \leq 1$ and $n/m \leq 1$ must be true all time. Unlike in Sporas formula, whenever a node is added to the network, it is given a reputation value equals to 1, means the reputation value is 100%. The reputation R must be calculated in fixed intervals. After few intervals, the average reputation value will be generated (includes the initial value). The average reputation value R_{av} should not fall below the threshold T . Therefore, it follows that $R_{av} > T$, otherwise the node is treated as malicious. Consider an arbitrary variable x that has a maximum value 1 and minimum 0. The current reputation value of a node is calculated as:

$$R_r = ((1-x).R_p + x.R_c) \leq 1 \tag{4}$$

where, R_r is the calculated reputation calculated, R_p is the previous reputation value, and R_c is the current reputation value. The value of x will be above 0.5 and closely the threshold value (0.95). The new updates must be small enough to be comparable with Sporas formula. The equation (4) will be compared to the equation (1), where the reputation in both cases provides the current trust status of the node. The average of these two values will provide best possible trust value R. Therefore,

$$R = (R_i + R_r)/2 \leq 1 \qquad (5)$$

If the node A observes that the node D is suspicious, Figure 1, then it broadcasts to its neighbor nodes C and B. The node C and node B calculates the trust value of node D using the broadcasted value and determines the node A's claim of suspiciousness. The node B calculates the trust of node D as below:

$$T_{ND} = R.R_{BA} + (1 - R_{BA}).R_{BD} \qquad (6)$$

where

T_{ND} is the new trust value of D at B

R is the trust value received from A

R_{BA} is the trust value of B on A

R_{BD} is the trust value of B on D

If A broadcasts that D is suspicious, B should not believe immediately. It should use the trust on A and trust on D and calculate the combined trust. If the calculated value is below the threshold then B believes that D is suspicious otherwise it broadcasts that D is not suspicious. Similarly the node C calculates its own trust on D.

Discussion of Results

We assume that the current trust value of node D is known by nodes A, B, and C. Suppose the current trust values of node D at nodes A, B, and C are 0.8, 0.85, and 0.92 respectively. Let *x*=0.8, and let R_r, R, and T_{ND} be given by equations (5) and (6). The value of R_r, R, and T_{ND} with respect to node C and node B decides that either node D will be trusted or not.

It is a known fact that sensors have limited resources including battery, computational, and communication resources. Therefore, it is suggested to use either Sporas formula or reputation-based trust model. It is further suggested using average of both formulas depending upon the sensitivity of the problem. If the data sensitivity is low and data need to be transferred securely then use either one of the formulas.

6. Simulations on Reputation-based Trust calculation

The simulation uses the Dynamic Source Routing (DSR) protocol of wireless sensor network. The simulation is written in the Java language. The idea of the simulation is based on the popular simulation software NS-2 (Network Simulator 2). We created a 500 x 500 field and randomly distributed 20, 50 and 100 nodes in the network. The simulation detected all misbehaving (nodes which did not forward data properly) nodes such as a sink hole and selective forwarding nodes. We calculated the trust ratio using promiscuous mode overhearing the packets forwarded by the successive node. The node swaps from promiscuous mode to normal mode as soon as it overhears the packet to save battery life. If it does not overhear packet for a given time frame, it automatically comes back to normal mode. The trust ratio was calculated using the number of packets received by successive node and transferred from it.

The sample simulations are given in Figure 3. We assumed node 2, node 3, and node 4 are neighbors of node 1. These four nodes transfer the data from the same node and calculate the reputation value. If the reputation value of node 1 drops below the threshold, then node 1 verifies the data from its neighboring nodes (nodes 2 – 4). For example, node 2 is a neighbor of node 1 and sent 50 packets and the successive node forwards 50 packets. That is 90% success. Similarly, the calculations follow from other nodes. Each node calculates its trustworthiness using equation (6) and send to node 1. The node 1 decides the trustworthiness of its successive after receiving data from its neighboring nodes.

7. Trust Cluster Approach

Trust clusters are very useful in the collaborative approach. The nodes within communication distance forms a cluster, and conduct collaborative activity in calculating the trust of any successive node. For example, if n_j is a neighbor of node n_i then we represent the neighbors $(n_i, n_j) = true$. Suppose, if n_i has more than one neighbor then we write

$$(n_i, n_j)_{\bar{\lambda} j} = true. \qquad (7)$$

$\bar{\lambda} j$ are the j nodes which are within the communication distance of node i. That is, i has the collaborative relation to the $\bar{\lambda} j$ nodes. Similarly, we form the neighboring nodes to each node in the network. Suppose $\zeta_{i,j}$ is the trust factor of each of j node close i^{th} node, then most dependable node in the neighborhood of a node i is the highest reputation value calculated through equation (5).

It is always necessary to keep track of the most trusted nodes within the communication distance and most inferior nodes within the communication distance. The inferior nodes will be eliminated to calculate the trust factor and if the trust factor of any inferior node is below the threshold, then all neighbors must discord the suspected node from the network. The inferior node is denoted as

$$\varsigma_{\inf} = (n_i, n_j)_{\lambda_j < threshold} \qquad (8)$$

Therefore, the node i must depend upon the trusted neighbor nodes for the future path selection.

8. Conclusions

Sensors are organized in an open environment and injecting of bad nodes to corrupt the transmission is possible. Therefore, a secure transmission model is required to avoid the transmission through corrupted node. The traditional protocols use exchange and distribute the keys for trust evidence. The resource limitations in sensor networks obstruct the use of traditional tools including cryptographic models and intrusion detection packages for secure communications. Encryption, intrusion detection models, and authentication techniques limits the performance of nodes in WSNs. Encryption and authentication cannot prevent the malicious or misbehavior of the sensor nodes. After reviewing relevant sensor network models, we believed that proposed collaborative trust-based model will overcome the shortcomings in the current models.

In the proposed collaborative model, each node is each node is updated through ratings. The ratings are provided by the nodes transfer the packets through that node. The update of node ratings is done through Sporas formula. If the node rate is below the threshold, the previous node uses the cooperative effort through neighboring nodes. By using the cooperative and collaborative effort, we eliminate the suspicious node from the communication path. Preliminary results are presented using the rating of a node through Sporas formula.

The future work includes the agent-based trust model. Each cluster has an agent and agent relieves the computations of the nodes. All decisions will be taken at the agent.

ACKNOWLEDGEMENT

The research work was supported by the ONR with award No. N00014-08-1-0856. The first author wishes to express appreciation to Dr. Connie Walton, Grambling State University and Dr. S. S. Iyengar, LSU Baton Rouge for their continuous support.

REFERENCES

[1] Reddy, Y. and Selmic, R., “Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach”, IARIA- ICN 2011, January 23-28, 2011 - St. Maarten, pp. 218-223.

[2] Liang, Z. and Shi, W., “PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing”, 38 Hawaii Int. conf. on Systems Sciences, 2005, pp. 201-210.

[3] Aberer, A. and Despotovic, Z., “Managing trust in a Peer-2-Peer information system”, 10th International Conference on Information and Knowledge management, 2001, pp. 310-317.

[4] Generowal, S. and Srivastava, M., “Reputation-based Framework for high Integrity Sensor Networks”, 2nd ACM workshop on Security of ad hoc and sensor networks, 2004, pp. 1-36.

[5] Marmol, F. and Perez, M., “Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique”, Networking and Electronic Commerce Research Conference (NAEC), 2008, pp. 1-16.

[6] Momani, M. and Challa, S., “Survey of Trust Models in different Network Domains”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010, pp. 1-19.

[7] Chen, H., “Task-based Trust Management for Wireless Sensor Networks”, International Journal of Security and its applications, vol 3, 2009 (last accessed: May 24, 2011), URL: http://earticle.net/article.aspx?sn=105974)

[8] Chen, H., Wu, H., Hu, J. and Gao, C., “Event-based Trust Framework Model in Wireless Sensor Networks”, IEEE International Conference on Networking, Agriculture, and Storage, 2008, pp. 359-364.

[9] Chen, H., Wu, H., Hu, J. and Gao, C., “Agent-Based Trust Management Model for Wireless Sensor Networks”, 2008 International Conference on Multimedia and Ubiquitous Engineering, 2008, pp. 150-154.

[10] Boukerche, A. and Xu, L., “An agent-based trust and reputation management scheme for wireless sensor networks”, Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE, 28 Nov.-2 Dec. 2005, pp.1857-1861.

[11] Chen, H., Wu, H., Zhou, X. and Gao, C., “Agent-based Trust Model in Wireless Sensor Networks”, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007, pp. 119-124.

[12] Zhang, W., Das, S. K., and Liu, Y., “A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks”, 3rd annual IEEE communications on sensor and ad hoc communications and networks (SECON 06), 2006, pp. 60-69.

[13] Momani, M. and Challa, S., "Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks," submitted to *Ad Hoc Networks*, 2007, pp. 381-403.

[14] Marsh, S. P., “Formalising Trust as a Computational Concept,” PhD Thesis, University of Stirling, 1994.

[15] Zacharia, G., Moukas, A., and Maes, P., “Collaborative Reputation Mechanisms for Electronic Marketplaces”, Decision Support Systems, Volume 29, Issue 4, December 2000, pp. 7-29.

[16] Josang, A. and Ismail, R., “The Beta Reputation System”, 15th Bled Electronic Commerce Conference, 2002, pp. 1-14.

Graphs

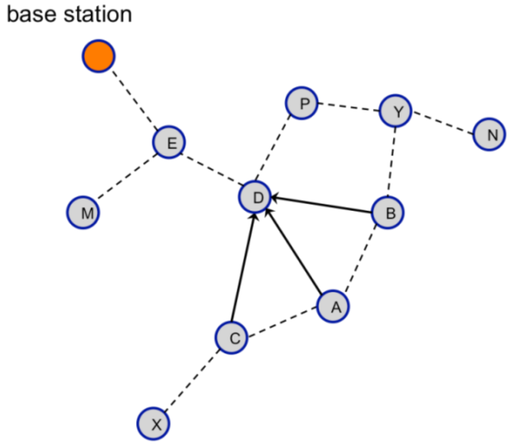


Figure 1. Wireless sensor network communication topology.

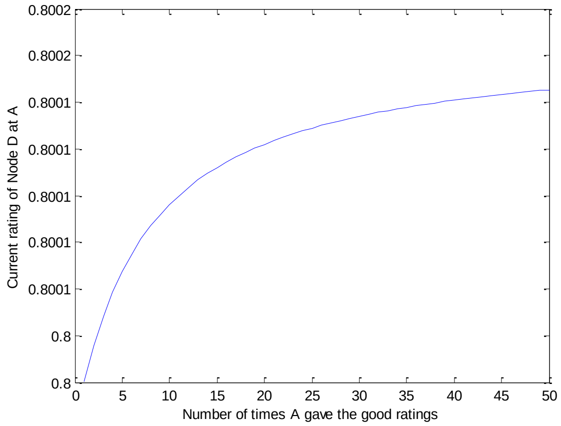
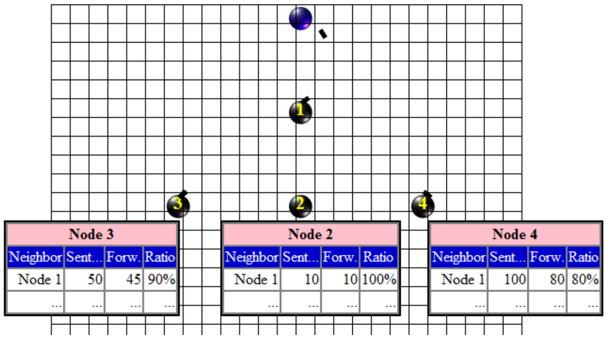


Figure 2. The rating of node A on node D.



Node 3			
Neighbor	Sent...	Forw.	Ratio
Node 1	50	45	90%
...	...	...	...

Node 2			
Neighbor	Sent...	Forw.	Ratio
Node 1	10	10	100%
...	...	...	...

Node 4			
Neighbor	Sent...	Forw.	Ratio
Node 1	100	80	80%
...	...	...	...

Figure 3: Simulation Of Wireless Sensor Networks using DSR Protocol

Copyright (c) IARIA, 2011. ISBN: 978-1-61208-144-1