ISBN: 978-1-4577-0750-6
IEEE Catalog Number: CFP1177H-PRT

Proceedings of the 2011 International Conference on Electrical Engineering and Informatics

July 17-19, 2011, Bandung-Indonesia

Volume 1

Organizer:

School of Electrical Engineering and Informatics
INSTITUT TEKNOLOGI BANDUNG, Indonesia

Co-Organizer:

Faculty of Information Science and Technology
UNIVERSITI KEBANGSAAN MALAYSIA, Malaysia

Sponsor:

IEEE

2011 International Conference on Electrical Engineering and Informatics

(ICEEI 2011)

Bandung, Indonesia
17-19 July 2011

Pages 1-924

IEEE Catalog Number: CFP1177H-PRT
ISBN: 978-1-4577-0753-7

TABLE OF CONTENTS

2011 International Conference on Electrical Engineering and Informatics
17-19 July 2011, Bandung, Indonesia

A Secure Trust Establishment in Wireless Sensor Networks

Farruh Ishmanov[1], Sung Won Kim[2]

Department of Information and Communication Engineering,
Yeungnam University, Gyeongsangbukdo, Korea

[1]farruh@ynu.ac.kr, [2]swon@yu.ac.kr

Abstract— **A functionality of wireless sensor networks depends on the cooperation of the sensor nodes in the network. A trust is major driving force to cooperate among sensors. Hence, trust establishment can be promising technique to improve network functionality. Moreover, trust establishment has been recognized as powerful tool to provide security. We propose a secure trust estimation method which does not allow malicious node to increase its trust value asrtificially. Unlike traditional trust estimation approaches, proposed scheme calculates trust on nodes based on only a bad behavior. Misbehavior of a node is weighted and based on the weighted misbehavior trust value is decreased. Since trust is dynamic nature, a node can increase its trust value if it does not misbehave. Numerical results demonstrate the effectiveness of the proposed trust estimation method.**

Keywords- ***trust establishment; security; misbehavior; wireless sensor networks***

I. INTRODUCTION

Recent developments in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have led to the introduction of sensor nodes which are small, low cost and capable of sensing, communicating and computing [1]. Collaboration of these sensor nodes comprises Wireless Sensor Network (WSNs). Since sensor nodes monitor the area in a cooperative manner and send an obtained data to base station (BS) by relaying each other, cooperation of the nodes is crucial. In order to maintain cooperation successfully, sensor nodes should choose trustful nodes to cooperate. Trust management(TM) evaluates the trustworthiness of a node and establishes trust relationships among nodes. Moreover, it forces nodes to collaborate with each other in a normal way to support the functions of the networks. Furthermore, as WSNs are vulnerable to many different adversary attacks [2], TM can enhance traditional security services by ensuring that all communicating nodes are trustful during authentication, authorization and key management [3]. From this point of view TM can improve cooperation between nodes and enhance security in the network.

Trust estimation is important part of the TM system (see Fig.1). By means of trust estimation method trustworthiness of nodes is evaluated. The scope of this paper is trust estimation part of the TM system. Trust can be estimated in two ways [4]:

1. Direct method based trust establishment.
2. Indirect method based trust establishment.

Direct method based trust establishment consists of the following steps:

1. Behavior of the node is monitored periodically;
2. In each period number of good and bad behavior of the node are recorded;
3. Based on the number of good and bad behavior trust is calculated periodically.

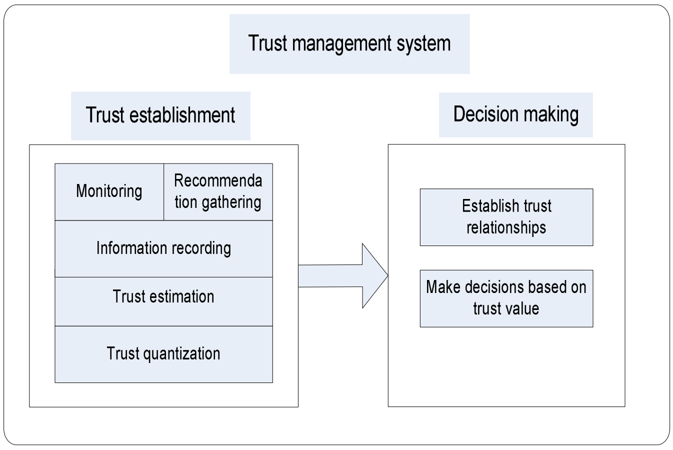

Fig. 1. Trust management system.

In indirect method based trust establishment nodes obtain recommendation from its trustful neighbors on the nodes. After receiving recommendations, trust is calculated based defined rules[8]. After trust estimation, nodes quantize trust values into different states and make decisions based on trust value.

As trust value determines the trustworthiness of the node, trust estimation method itself firstly should be accurate and secure. Otherwise, it leads to insecurity in the network and incorrect decisions on nodes. As stated above, conventional trust estimation methods determines trust based on the number of good and bad behavior of a node [5][6][7][8]. When the number of good behavior sufficiently large, significant number of bad behavior is concealed. Thus, it gives chance an attacker node to attack and be trustful at the same time by manipulating the number of good and bad behavior. Moreover, an attacker node can attack passively and show more good behavior in order to gain trust. Hence, considering good behavior in trust estimation should be reconsidered.

In this work, we propose a new secure approach to estimate trust. In order to estimate the trust we consider only bad behavior of the node so that malicious or attacker node can not manipulate with its number of good behavior. As in conventional trust estimation method behavior of the node is monitored periodically and during this period only bad behaviors of the node are recorded. After that misbehavior of the node is weighted by the proposed weighting mechanism. Based on the weighted misbehavior trust value is decreased. Since nature of the trust is dynamic [4], proposed trust evaluation method considers increasing trust of the node. If the node does not show any misbehavior for current time period then it can increase its trust value based on the proposed trust increasing mechanism.

The numerical results show that our trust establishment scheme can efficiently evaluate and detect malicious nodes. Moreover, it shows that proposed scheme is flexible and adaptive.

The remainder of the paper is organized as follows: Section II describes related work. Section III contains definitions, assumptions and proposed scheme. Section IV proposes evaluation results. Section V concludes this paper and suggests some future directions.

II. RELATED WORK

Trust management system in WSNs in its developing stage[5]. Although there are several works, few of them considering TM in great detail. Since trust management concept is new in digital world, modeling the digital trust for WSNs requires a lot of research. Trust establishment is part of trust management system. Although some of the stated schemes are trust management, it does have trust establishment part. So, we will focus on that part of the mentioned schemes (see Fig.1).

In [5] Reputation-Based Framework for High Integrity Sensor Networks (RFSN) is proposed. In this trust management scheme, each sensor node maintains the reputation for neighboring nodes only. The scheme is based on reputation system. Trust values are calculated on the basis of that reputation and Bayesian formulation for representing reputation of a node is used. Reputation metric is obtained based on node's ratings on the other node. It is assumed that it follows beta distribution and reputation probability defined as follows[5]:

$$P(\theta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \quad \forall \ \ 0 \le \theta \le 1, \quad \alpha \ge 0, \quad \beta \ge 0 \qquad (2.1)$$

α is number of good behavior, β is number of bad behavior Γ () is gamma function.

Trust metric *Tij* is node *i'*s prediction of the expected behavior of node *j* is obtained by taking a statistical expectation of reputation probability of node *j*[5];

$$T_{ij} = E[R_{ij}] = E[Beta(\alpha_j, \beta_j)] = \frac{\alpha_j}{\alpha_j + \beta_j} \qquad (2.2)$$

It is simply expectation value of beta distribution where α and β are number of good and bad behavior of node j. So the scheme considers both bad and good behavior in estimation of the trust as stated above.

In [6], Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks (GMTS) is proposed. GTMS calculates the trust value based on direct or indirect observations. Direct observations represent the number of successful and unsuccessful interactions and indirect observations represent the recommendations of trusted peers about a specific node. Timing window mechanism is used to avoid the time effect on trust value. The timing window *Δt* is used to count the number of successful and unsuccessful interactions. It consists of several time units. The interactions that occur in each time unit within the timing window are recorded. After a unit of time elapses, the window slides one time unit to the right, thereby deleting the interactions done during the first unit. Given information in time window, the time-based past interaction trust value *Tx,y* of node *y* at node *x* that lies between 0 and 100 is defined as [6]:

$$T_{x,y} = [100(\frac{(S_{x,y})^2}{(S_{x,y} + U_{x,y})(S_{x,y}+1)})] \qquad (2.3)$$

where [] is the nearest integer function, *Sx,y* is the total number of successful interactions of node x with y during time *Δt*, *Ux,y* is the total number of unsuccessful interactions of node x with y during time *Δt.*

As we can see here also good behavior is considered in trust estimation.

In[3] author proposed trust modeling against selfish and falsely accusing node behavior in distributed systems like WSNs. In order to estimate trust value of a node, firstly confidence level is determined as follows [7]:

$$C_{ij} = \frac{\sum_{Tav} \Delta_{rij}}{\sum_{Tav} \Delta_{fij}} \qquad (2.4)$$

where C_{ij} is confidence level of node *j* as computed by node *i*, $\sum_{Tav} \Delta_{rij}$ is summation of number of packets requested to forward by node *i* to node *j* over time period T_{av}, and $\sum_{Tav} \Delta_{fij}$ is summation of number of packets forwarded by node *j* requested by to node *i* over time period T_{av} .

After estimation, node *i* broadcasts its own estimated confidence level value of node *j*. Likewise node *i* receives the confidence level of node *j* by all of the nodes. So, node *i* and other nodes integrate all received confidence level for node *j*, as follows [7]:

$$C_j = \frac{1}{N-1}\sum_{i \ne j} C_{ij} \qquad (2.5)$$

where N = number of considered nodes.

In this way every node dynamically updates the confidence level of all its neighbors. This is stored as a scalar matrix. For node *i* it is denoted as:

$[C_1^{i}C_2^{i}C_3^{i}....C_K^{i}]$, where *1, 2, ..., K* are the neighboring nodes of node *i*. This matrix is updated periodically with *Tav* as the time period.

Now, after computing the confidence level of its neighbor all the nodes compute the trust of its neighbor, which is[]:

$$[C_1^{i}-C_T\ \ C_2^{i}-C_T....C_K^{i}-C_T]=[T_1^{i}\ \ T_2^{i}....T_K^{i}] \qquad (2.6)$$

where C_T is predefined confidence threshold $T_K^{\,i}$ is the trust level of node *K* by node *i*.

If some malicious node falsely accuses other legitimate node as selfish node, then accused node records it as follows[7]:

$$A_j^{\,i}=\begin{cases}0; if\ j\ accuses\ i\ falsely\\ 1; if\ j\ reward\ i\ for\ forwarding\end{cases} \qquad (2.7)$$

Accordingly, node *i* updates its confidence value for node *j* as[7]:

$$C_{ij}=\frac{\sum_{Tav}\Delta_{rij} * A_j^{\,i}}{\sum_{Tav}\Delta_{fij}} \qquad (2.8)$$

So, in this case confidence level of node *j* becomes zero. In this way accuser node is punished and its trust value is decreased.

As it is stated above confidence level of a node is estimated based on number of forwarded and requested packets, which allow malicious node manipulate with number of forwarded and requested packets.

Effects of considering a good behavior in trust estimation

There are several problems related to considering of legitimate behavior in trust estimation**.** We show these issues by example and this is based on GMTS[6]**.**The first problem is *inconsistent trust value.* In the Fig.2 below *y* axis shows the trust value and number of misbehavior by node A on node B and *x* axis shows the timeline. A trust is computed based on GMTS [5]. As we can see in the Fig.2, although the number of bad behavior is five during the first and the second time a trust value is different. Thus, even nodes' number of misbehavior is the same a trust value of those nodes will be different which is not reasonable.

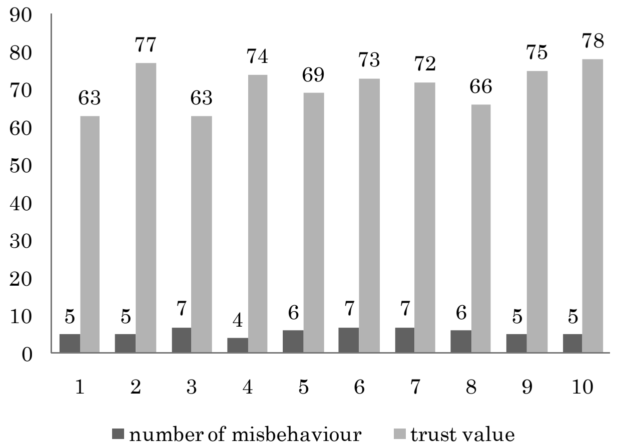

Fig. 2 An inconsistent trust value.

The second problem associated with trust estimation considering number of good behavior is incorrect trust value. When the number of good behavior increases of the node, its trust value also increases even though a node has a significant number of misbehavior if it has certain amount of good behavior it will gain high trust value. As it is demonstrated in Fig.3, although a number of misbehavior significantly large (8~14), node B has a good trust value according to GMTS. The number of good behavior is in the range of [35; 50]. So in this case a node B is considered trustful even though it acts greatly as malicious node.

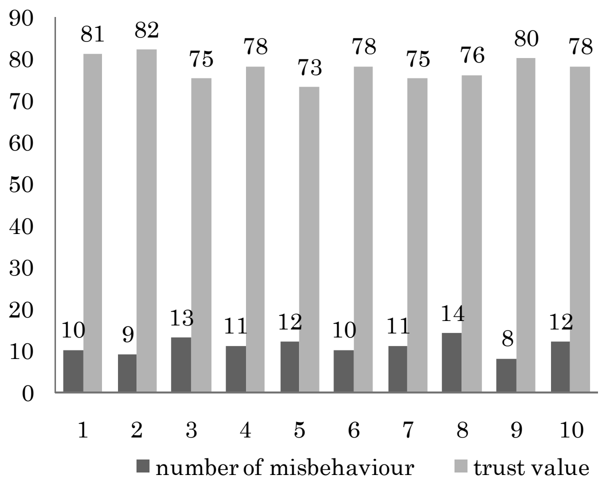

Fig. 3 An incorrect trust value.

Although there is no chance for attacker node A to increase its number of good behavior so that it can manipulate with it, still node *A can attack passively* and can show itself as a trustful node (see Fig.4). The number of good behavior is in the range of [6;14].

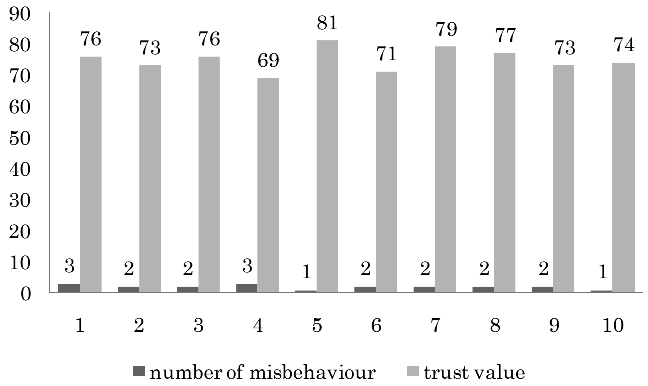

Fig. 4 An incorrect trust value in case of passive attack.

As the figures prove considering good behavior in the calculation of trust causes serious problems such as increasing trust value artificially or incorrect trust value, obtaining inconsistence trust value and leaving room for passive attack.

III. SECURE TRUST ESTABLISHMENT SCHEME

In this section we present description of the proposed trust establishment scheme. Firstly, to estimate the trust, misbehavior of the node is weighted by the proposed weighting mechanism, which considers only bad behavior of the node. Then based on the weighted misbehavior trust value is decreased. If a node does not show any misbehavior for current time period then the trust value is increased based on the proposed trust increasing method.

The following assumptions are made for the scheme:

1. In the initial state all nodes have trust value of 70 which is the lowest threshold of the trusted zone;
2. Every t_k period nodes estimate trust for their one-hop neighbors. If node needs trust value for other than one hop node, it establishes trust based on recommendation method.
3. The maximum trust value is 100.

In order to estimate trust of Node B, node A weights misbehavior of node B as follows:

$$M_{t_k}^{A,B} = (\alpha+\beta) * \left[10 * \left(\frac{m^B}{\sum_{i=1}^{n} m^i} \right) + m^B \right] \quad \alpha \le 1\ ,\ \ \beta \le 1 \quad (3.1)$$

Since network condition and sensor node capability can effect on trust value, α is for the mitigation of the effects of the network condition and sensor node error. β is weighting parameter. It can be adaptive depending on the situation in the network. The higher it is, the faster trust value is decreased. m^B is number of misbehavior during the time t_k, $\sum_{i=1}^{n} m^i$ is summation of misbehavior of neighbors of node A. $m^B / \sum_{i=1}^{n} m^i$ is to determine the contribution of node B to overall misbehavior. It is to avoid active misbehaving nodes. Since active attacker node can destroy network in a short time, considering contribution this factor in weighting of misbehavior can faster avoid such an active attacker node.

After weighting the misbehavior of node B, trust for node B is estimated as follows:

$$\text{If} \quad M_{t_k}^{A,B} > 0, \qquad T_{t_k}^{A,B} = T_{t_{k-1}}^{A,B} - M_{t_k}^{A,B} \qquad (3.2)$$

where $T_{t_{k-1}}^{A,B}$ is trust value of node B in t_{k-1} time. As node misbehaves its trust value decreases by the time as indicated in the equation 3.2.

If node does not misbehave for the current time t_k and its trust value lesser than 100, then it can increase its trust value:

$$\text{If} \quad M_{t_k}^{A,B} = 0, \quad and \quad T_{t_{k-1}}^{A,B} < 100$$

$$T_{t_k}^{A,B} = T_{t_{k-1}}^{A,B} + \chi * \left[\frac{\max T - \sum_k M_k^{A,B}}{10} \right] \qquad (3.3)$$

where *maxT* is maximum trust value that is 100, $\sum_k M_k^{A,B}$ is the summation of the last k weighted misbehavior of node B. k can be adaptive, but the more it is, the more accurate trust value is obtained. However, more k requires storing more historical weighted misbehavior which requires more memory space. So, there is tradeoff between the number of weighted misbehavior and accuracy of the trust value. Node can increase its trust value as long as he does not misbehave. It shows the flexibility and fair estimating property of the proposed scheme. It is fair to decrease trust if node shows misbehavior and to increase trust when node does not misbehave. Also, it makes trust establishment scheme more flexible and dynamic.

In brief, idea behind the scheme as follows: all the nodes are in the very beginning of the network considered to be trustworthy; if a node misbehaves, it is trust value is decreased based on its weighted misbehavior; on the other hand if node is legitimate, it is trust value is increased up to 100 gradually.

After calculating the trust values nodes can be quantized trust into five states as stated in Table 1.

TABLE I. Trust states.

Trust value	**State**
$85 \le x \le 100$	Trustworthy
$70 \le x < 85$	Less trustworthy
$55 \le x < 70$	Untrustworthy
$0 \le x < 55$	Highly untrustworthy

IV. Evaluation Results

In this section, we present numerical results and comparison of the proposed scheme with other schemes. For the sake of the simplicity only two nodes considered. Node A estimates trust value for his neighbor node B based on his number of good and bad behavior which are generated randomly in certain range. The fig.5 shows trust evaluation comparison among GMTS, RFSN and proposed scheme.te malicious nodes. In the estimations, parameters in proposed scheme α and β are 0.2. Number of good behavior ranges from 37 to 49 and number of bad behavior ranges from 8 to 14 in each trust estimation method. As graph shows performance of GMTS and RFSN is similar in which trust values and trust probabilities are within the trusted zone.

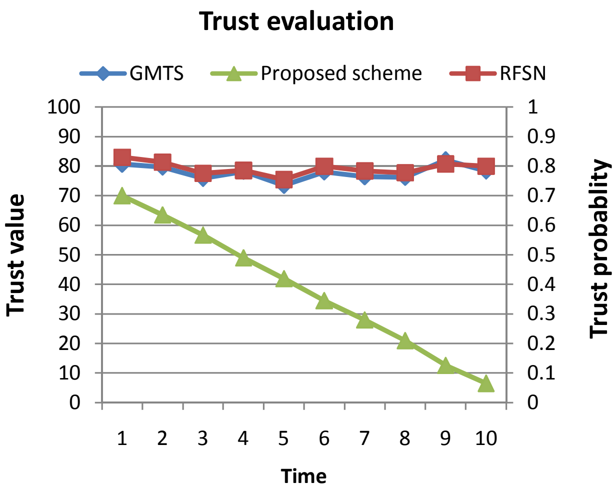

Fig. 5 Trust evaluation in case of an active attack.

As we can see in the graph trust value is decreasing abruptly in the proposed scheme since node actively misbehaving in each time period. Since this kind of node can destroy network in a short period or degrade network performance significantly, it should be detected and avoided. The reason why other schemes can not detect such kind of misbehavior is that node shows about forty good behaviors which conceals its bad behaviors. Now we assume that malicious node does not have chance to show large number of good behavior such forty times or more so that it can attack efficiently. The Fig.6 shows that even in this case malicious node can still misbehave and gain trust by passively attacking in the previously proposed schemes. In this case number of good behavior ranges from 6 to 14 and number of bad behavior is between 1 and 3. As we can see GMTS shows lower trust values than that of RFNS but still it's between 70 and 80. On other hand, proposed scheme shows decreasing trend in trust value as time passes even though misbehavior is small number.

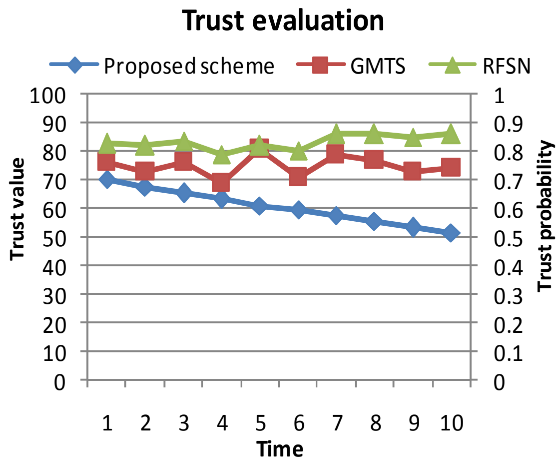

Fig. 6 Trust evaluation in case of passive attack.

Note that we assume that a node with high trust value such as 80 out of 100 or 75 out of 100, it is trustworthy. On the other hand, trust value below 50 or 60 shows that it is not trustworthy. Next we compared trust schemes in case where attacker or malicious node attacks more in an intelligent way. In this kind of attack attacker node attacks for some time and behaves good to gain trust for another time. As we can see misbehavior node first shows misbehavior and then does not show any misbehavior for some time and then it again shows misbehavior (see Fig.7). In this case number of good behavior is fixed that is 16. The results demonstrate that although node is malicious it gains high trust value even in attacking period in previously proposed schemes. On other hand, our proposed scheme shows more stable trust value. Depending on the number of misbehavior, trust is increased and decreased. So, proposed scheme shows the balance between increasing and decreasing which assists to evaluate the trustworthiness more accurately. As we can see in the proposed scheme trust values are kept within the untrustworthy zone (see Fig.7).

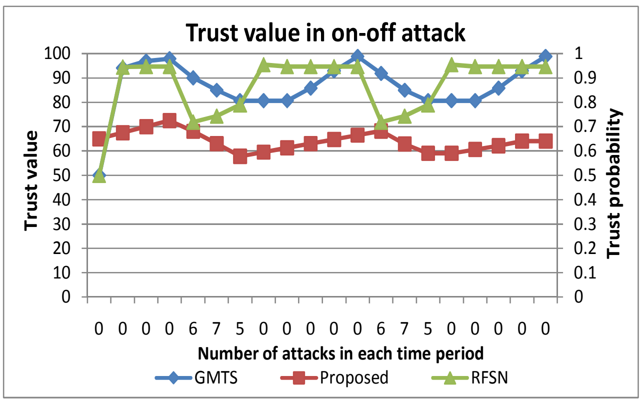

Fig. 7 Trust evaluation value in case of on-off attack.

V. CONCLUSIONS

This paper presents a novel trust establishment scheme. The issues related with considering good behavior in trust estimation are demonstrated. The scheme establishes the trust based on only misbehavior of the node which makes trust establishment scheme more secure. Furthermore, if node does not show misbehavior, trust value will be increased based on proposed mechanism. Numerical results validate the effectiveness of the proposed scheme.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, no. 4, 2002, pp. 393–422.

[2] W. Zhang, S.K Das, Y Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless", Proceedings *of the Sensor Networks Sensor and Ad Hoc Communications and Networks, 2006. SECON '06*

[3] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications", IEEE *Comm. Surveys and Tutorials, vol. 3, no. 4, 2000.*

[4] R. Subramanian, "Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions", IGI Gloabal, Pages: 1-356 pp. 2008

[5] S. Ganeriwal and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 66-67, Oct. 2004.

[6] R. A Shaikh, H Jameel, Brian J. d'Auriol, H Lee, S Lee, Y J Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks", *IEEE Transaction On Wireless Comm*., Vol. 1, No. 4, 2009.

[7] Ukil, Arijit. "Secure Trust Management in Distributed Computing Systems", *Proceedings of Electronic Design, Test and Application (DELTA), 2011.*

[8] Yan Sun, Wei Yu, Zhu Han, and K. J. Ray Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", *IEEE JSAC special issue on security in wireless ad hoc networks, Vol 24, no.2, February, 2006*