Int. J. Advanced Networking and Applications 1951
Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290

Design of Dependable and Trustworthiness Of Data Communication In WSN

R.Satheeskumar
Head of the Department Computer Science and Engineering, Bharath Niketan Engineering College,
Email: satheesme@gmail.com
B.Anbuselvan
Assistant Professor Computer Science and Engineering, Bharath Niketan Engineering College,
Email: selvananbume@gmail.com
M.Kasipandi
Department of Computer Science,Bharath Niketan Engineering College
Email: kasipandi1985@gmail.com

----------ABSTRACT----------

This work discusses a novel of the most challenging issues so far is the extension of network lifetime with regards to small battery capacity and self-sustained operation. Endeavors to save energy have been made on various frontiers, ranging from hardware improvements over medium access and routing protocols to network clustering and role changing strategies. In addition some authors studied failures in communication regarded as error detection First, a lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. Due to canceling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system ef iciency while reducing the effect of malicious nodes. More importantly, considering that CHs take on large amount of data forwarding and communication tasks, a dependability-enhancedtrust evaluating approach is defined for cooperations between CHs. This approach can effectively reduce networking consumption while malicious, selfish, and faulty CHs. Moreover, a self-adaptive weighted method is defined for trust aggregationat CH level. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assignesubjectively. Theory as well as simulation results shows that LDTS demands less memory and communication overhead compared with the current typical trust systems for WSNs.

Keywords: **Reputation, self-adaptivity, trust management, trust model, wireless sensor network.**

Date of Submission: December 03, 2013 Date of Acceptance: December 30, 2013

1. Introduction

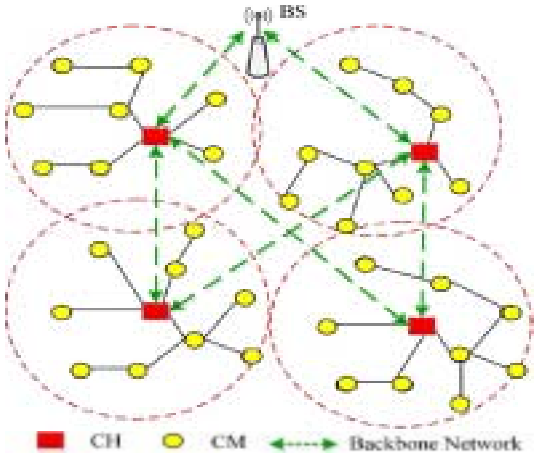
To the best of our knowledge, we are the first to conduct a systematic study of a trust management system for clustered WSNs from the perspective of both dependability and resource efficiency. The key features of LDTS go beyond existing approaches in terms of the following aspects:

1) *A lightweight trust evaluating scheme for cooperations between CMs or between CHs*. Within the cluster, the indirect trust of a CM is evaluated by its CH. Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of a bad-mouthing attack by compromised CMs. The feedback of a CH is applied a similar manner to obtain the same benefits.

2) *A dependability-enhanced trust evaluating approach for cooperations between CHs*. Considering that CHs take on large amounts of data forwarding and communication tasks, a dependability-enhanced trust evaluating approach is defined for cooperations between CHs. This approach can effectively reduce networking consumption while preventing malicious, selfish, and faulty CHs.

3) *A self-adaptive weighting method for CH's trust aggregation*.
This approach overcomes the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively.

Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290



Roles and identities of nodes in a clustered WSN model

2.Lightweight Scheme for Trust Decision-Making

Our proposed LDTS facilitates trust decision-making based on a lightweight scheme. By closely considering the identities of nodes in clustered WSNs, this scheme reduces risk and
improves system efficiency while solving the trust evaluation problem when direct evidence is insufficient (See Section IV-B).

This scheme is described as follows:

2.1 Trust Decision-Making at CM Level:

A CM calculates the trust value of its neighbors based on two information sources direct observations (or direct trust degree, DTD) and indirect feedback (or indirect trust degree, ITD). DTD is evaluated by the number of successful and unsuccessful interactions. In this work, interaction refers to the cooperation of two CMs. All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if node sends a message to CH via node , then node can hear wether node forwarded such message to CH , the destination. If does not overhear the retransmission of the packet within a threshold time from its neighboring node or if the overheard packet is found to be illegally fabricated (by comparing the payload that Trust decision-making at CH level. is attached to the packet), then will consider the interaction unsuccessful. Unlike most existing reputation or trust models, which rely on broadcast-based strategy to collect feedback from the whole cluster, consequently increasing the system communication overhead significantly, our LDTS does not utilize a broadcast- based strategy and instead sets the value of ITD is based on the feedback reported by the CH about a specific node. Thus, each CM does not need to share trust information with its neighbors. This indirect feedback mechanism has numerous advantages such as the effective mitigation of the effect of malicious feedback, thereby reducing the networking risk in an open or hostile WSN environment. Given that the feedback between CMs need not be considered, this mechanism can significantly reduce network communication overhead, thus improving system resource efficiency. As an example of trust decision-making at the CM level, if a node wants to communicate with node, first checks whether it has any past interaction records with during a specific time interval. If a past interaction record exists, then makes a decision directly; otherwise, will send a feedback request to its CH.

2.2 Trust Decision-Making at CH Level: In cluster WSNs, CHs form a virtual backbone for intercluster routing where CHs can forward the aggregated data to the central BS through other CHs. Thus, the selection of CHs is a very important step for dependable communication. In our LDTS, the GTD of a CH is evaluated by two information sources *CH-to-CH* direct trust and *BS-to-CH* feedback trust. During *CH-to-CH* communication, the CH maintains the records of past interactions of another CH in the same manner as CMs keeps interaction records of their neighbors. Thus, the direct trust value can be computed according to the number of successful and unsuccessful interactions. The BS periodically asks all CHs for their trust ratings on their neighbors. After obtaining the ratings from CHs, the BS will aggregate them to form an effective value of ITD.

Similar to the trust decision-making process at the CM level, in our LDTS, the ITD of a CH only depends on the feedback reported by the BS. Thus, in the CH-to-CH communication case, when a CH wants to interact with another CH , it will send a feedback request to the BS, at the maximum. Therefore, including the response message form the BS, the total communication overhead is two packets. Thus, this mechanism can also greatly reduce network communication overhead and consequently improve the system's resource efficiency. Compared with trust decision-making at the CM level, trust decision-making at the CH level has to calculate for direct trust and feedback trust simultaneously. As an example of trust decision- making at the CH level, if a CH wants to communicate with another CH, first calculates CH-to-CH direct trust for based on the past interaction records with during a specific time interval. Meanwhile, sends a feedback request to the BS. After receiving the request, the BS will send a response message to , in which 's feedback trust value (BS-to-CH feedback trust) is embedded. Then, will aggregate these trust sources into a GTD, after which will make a final decision based on's GTD.

3. LIGHTWEIGHT AND DEPENDABILITY-ENHANCED TRUST CALCULATION

The domain of trust values has the Following benefits:

1) *Less memory overhead*. An unsigned integer between 0 and 10 only needs 4 bits (0.5 bytes) of memory space, thus

Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290

saving save 50%memory space compared with trust values represented as an integer between 0 and 100 (1 bytes) and 87.5% compared with trust values represented as a real number (4 bytes).

2) *Less transmission overhead*. Given that a smaller number of bits require transmission during the exchange of trust values between nodes, we gain the benefit of less overhead of transmission and reception power.

3.1Dependability-Enhanced Intercluster Trust Evaluation

In accordance with the characteristics of clustered WSNs, both CMs and CHs are resource-constrained nodes, and BSs have more computing and storage capacity and no resource constraint problem. Thus, energy conservation remains a basic requirement for trust calculation at CHs. In LDTS, we propose a dependable and energy-saving scheme, which is suitable for large-scale and clustered WSNs.

4. THEORETICAL ANALYSIS AND EVALUATION

i) Dependability Analysis against Malicious Attacks

In this section, we analyze the dependability of the LDTS protocol against attacks on a trust management system. In clustered WSNs, the main attacks from a malicious node primarily include two kinds of patterns:

1) *Garnished attack.* In such an attack, malicious nodes behave well and badly alternatively with the aim of remaining undetected while causing damage. For instance, garnished malicious nodes may suddenly conduct attacks as they accumulate higher trustworthiness.

2) *Bad mouthing attack.* As long as feedback is considered, malicious nodes can provide dishonest feedback to frame good parties and/or boost trust values of malicious nodes. This attack, referred to as the bad mouthing attack [6], is the most straightforward attack. After providing evidence of the malicious nodes' objectives, we can prove that our trust management system at both the CM and CH levels is dependable against attacks from malicious nodes because this system can detect the malicious behavior and can prevent such nodes from fulfilling their objectives. We broadly categorize two types of nodes (CMs or CHs): Good ones and malicious ones. Our assumption is that good nodes interact successfully most of the time and submit true feedback. Conversely, malicious nodes try to launch garnished attacks or bad mouthing attacks. In Section VI, we define this concept more rigorously, capture the behavior of malicious nodes, and model how such nodes might try to gain an unfair advantage in our trust scheme. Then, we prove our trust system's dependability against such malicious attacks.

ii). Communication Overhead Analysis and Comparison

To evaluate the communication overhead under full-load conditions, we assume a worst-case scenario which is similar to [8], in which every CM wants to communicate with every other CM in the cluster, and every CH wants to communicate with the rest of the CHs in the network. At the same time, each CH needs to collect feedback reports from its CMs, and the BS has to collect feedback reports from its CHs. Let us assume that the network consists of clusters and that the average size of clusters is (including the CH of the cluster). In intracluster trust evaluation, when node wants to interact with node, node will send a maximum of one CH feedback request, for which node will receive one response. If node wants to interact with all the nodes in the cluster, the maximum communication overhead will be . If all nodes want to communicate with one another, the maximum communication overhead is .When a CH wants to collect feedback from its members, it will send requests and receive responses, thus resulting in a total communication overhead of

Thus, the maximum intra cluster communication overhead is $C_{inter}=2(m-1)(m-1)+2m=2(m1)^2+2m$.

5. STORAGE OVERHEAD ANALYSIS AND COMPARISON

Each CM has to maintain a small trust database, as shown in The size of each record is 7 bytes. Therefore, the storage requirement for LDTS at each CM is bytes, where represents the number of CMs in a cluster. The size of the trust table mainly depends on the size of the cluster. Each CH maintains two tables, one of which is used to store the feedback matrix (see (2)), thus resulting in a total storage overhead of . In the second table, each CH maintains a trust database as shown in The size of each record also is 7 bytes. Therefore, storage requirement for CHs is bytes, where represents the number of CMs in a cluster. The total storage overhead at the CH for both tables is .The formulas for the storage requirements of three trust management systems LDTS, GTMS, and ATRM, are given in Table II, in which represents the average number o in each cluster, represents the total number of CHs in the network, is the time window defined by GTMS, and represents the number of contexts described in ATRM (for details about the storage requirements of GTMS and ATRM, please see [8]). and 9 show the storage overhead of three trust management systems under a clustered WSN environment, which has a total of 1,000 nodes. On the whole curve of we can see that our LDTS needs less storage overhead than the two other trust systems, GTMS and ATRM. This condition proves that LDTS at the CM level consumes less memory than the two other models. Shows that as the number of clusters increases in the network, the LDTS introduces less storage overhead at the CH level compared with the two other systems, which indicates that LDTS is more suitable for large-scale WSNs having a small size of clusters. The results in can be easily explained by Table II. In LDTS,

Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290

the total storage overhead at the CH level is bytes. Evidently, the value
of primarily depends on the number of nodes at each cluster. As the number of nodes at each cluster increases, the storage consumption requirement also increases at the CH. As the number of nodes at each cluster decreases, the storage consumption requirement also decreases linearly at CH

6. SIMULATION-BASED ANALYSIS AND EVA L U AT I O N

By extending the Netlogo-basedtrust simulation engine [23],[28], we implemented a simulator to test the feasibility of the proposed LDTS. For the purpose of comparison, we also added GTMS [8] into the simulator, because both LDTS and GTMS are independent of any specific routing scheme and platform. We did not implement the ATRM system [20] because it requires a specific agent-based platform.

A. LDTS Simulator and Environment

In the simulator, three kinds of nodes exist based on their identities (Table III), i.e., as a CM, as a CH, and as a BS. A CM or a CH can be a collaborator or a rater toward other nodes. The behavior of a CM as a collaborator can be one of two types: good CM (GCM) and bad CM (BCM). GCMs will provide successful interaction for the requested messages, whereas BCMs will provide an unsuccessful interaction. The behavior of a CM as a rater can be one of two types: honest CM (HCM) and malicious CM (MCM). An HCM always gives the appropriate rating for any CM, whereas an MCM always gives a random rating between 0 and 10 for other CMs. Similar to a CM, a GCH always provide successful interaction, whereas a BCH provide an unsuccessful interaction. An HCH always gives an appropriate rating, whereas an MCH always gives random rating between 0 and 10. Based on discussions in Section III and IV, we can see that LDTS works with two topologies: the intercluster (CH-to-CH) topology, where distributed trust management is used, and intracluster (CM-to-CM) topology, where the centralized trust management approach is employed. We alsofind that different calculation mechanisms are employed for intracluster and intercluster trust evaluations. According to these characteristics of LDTS, in this simulator, we separately evaluate the performance of LDTS based on intracluster and intercluster cases. This approach will not affect the results of performance evaluation and will greatly reduce the complexity of the simulator. Instead of using the physical running time, we use the notion of time-step,which is introduced in Netlogo, to calculate the simulation time.The simulation parameters and default values used in the experiments are listed in Table IV.

B. Overhead Evaluation and Comparison

We aim to study the effect of the trust management system in a WSN community, which closely resembles a real network environment. We suppose that most CMs and CHs are good, where only 20% CMs and CHs are malicious. The comparison results are shown in With the increasing the number of CMs in a cluster, the CM-to-CM communication overhead of GTMS rapidly increased according to a exponential curve. However, the CM-to-CM communication overhead of LDTS slowly increased with the increasing number of CMs. This finding further confirms our conclusions from the theoretical analysis in Section VI, that is, given that feedback between CMs need not be considered, this trust calculation mechanism in LDTS can greatly reduce communication overhead. show the comparison results of the CH-to-CH communication overhead between LDTS and GTMS. LDTS and GTMS have a relatively close network overhead as the network size increases, which indicates that both LDTS and GTMS are suitable for large-scale clustered WSNs. However, by comprehensively analyzing the results in LDTS is more suitable for large-scale clustered WSNs with a large size of clusters, thus outperforming GTMS. The comparison results of average storage overhead at each CM in a cluster. With the increasing number of CMs in a cluster, the average storage overhead of GTMS gradually increased according to a linear curve. However, the average storage overhead of LDTS was less than a third of that of GTMS and slowly increased with the increasing number of CMs. This finding confirms our conclusions from the theoretical analysis in Section VI. The average storage overhead of the two trust systems at each CH in a WSN network having an equal size f clusters (10 nodes). We find that as the number of clusters increases in the network the GTMS introduces slightly less storage overhead compared with LDTS. The results in can be easily explained by (2). Each CH has to maintain an additional table, which is used to store the feedback matrix (see (2)). The total storage overhead is . Although the introduction of matrix increases the storage overhead of a CH node, this matrix can significantly enhance the dependability of CH-to-CM trust evaluation.

C. Dependability Evaluation and Comparison

We compute the packet successful delivery ratio(PSDR) to reflect the dependability of trust management systems. A higher PSDR indicates higher dependability. We suppose that most CMs and CHs are good in the WSN community, where BCMs and BCHs each comprise only 10%. This WSN environment closely resembles a real situation, where most CMs are honest and most CHs are good. The PSDR comparison results under different percentages of malicious cluster heads (MCHs). In this group simulation, we suppose that in the WSN community, where 95% of CMs are honest. The remaining 5% of CMs are MCMs. We separately set the percentage of MCHs as 5%, 10%, and 20%, which respectively indicate that the WSN environment is honest, relatively honest, and dishonest community, with 50,100, and 200 dishonest CHs separately. An honest WSN environment, where the

Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290

percentage of MCHs is only 5%. We can see that both LDTS and GTMS have a high PSDR, which reflects that these two models have a high dependability under an honest WSN environment. In and the simulation results when MCHs is 10% and 20% have larger differences compared with . With the increase in the percentage of malicious CHs, the performance of both LDTS and GTMS show a marked decline. Relatively, LDTS has a robust performance under a dishonest WSN environment. These results are consistent with a real situation, i.e., in a dishonest WSN community, malicious CHs may conduct a bad-mouthing attack, which can greatly affect the performance of the WSN system. To reduce the risk of trust evaluation, we adopt the idea that the GTD of a CH is adaptively merged by two parts (which is not aggregated by GTMS):CH-to-CH direct trust and BS-to-CH feedback trust. This can significantly improve the dependability of LDTS. Shows the PSDR comparison results under different percentages of MCMs. We find that LDTS also has a more robust dependability than the GTMS scheme. Shows the experimental results under an honest environment. In the simulation, the total percentage of MCMs is 10%, and the total percentage of MCHs is likewise 10%, which indicate that the community is a relatively honest community (i.e., with fewer MCHs and MCMs). Both LDTS and GTMS have relatively stable performance within 1,000 time-steps, even if their PSDRs change from 0.92 to 0.96. Shows the experimental results under a relatively honest environment, where 20% of CMs are dishonest. The results show that LDTS has a higher PSDR than GTMS. The experimental results under a highly dishonest environment, where 30% of CMs are dishonest. Under this case, LDTS still shows better dependability than GTMS.

7. SIMULATION AND RESULTS

In this (Fig7.1, Fig7.2) result, to propose LDTS for clustered WSNs. Given the cancellation of feedback between nodes, LDTS can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperation's between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Theory as well as simulation results show that LDTS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

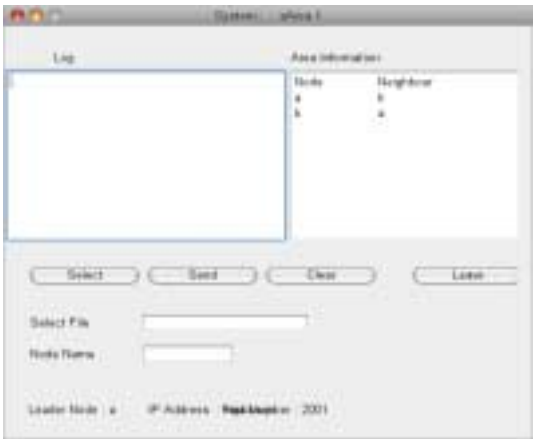


Fig 7.1

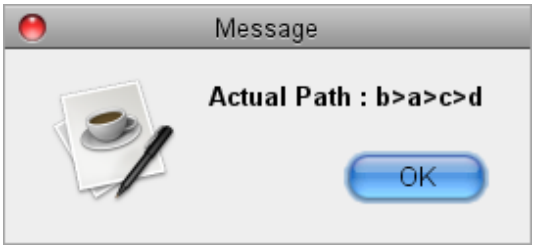


Fig 7.2

8. CONCLUSION

In this work, we proposed LDTS for clustered WSNs. Given the cancellation of feedback between nodes, LDTS can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperation's between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Theory as well as simulation results show that LDTS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

REFERENCES

[1] W. B. Heinzelman, A. P. Chandrakasan, andH. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks,"*IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670,Oct. 2002.

[2] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Comput. Commun.*, vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," *IEEE Trans.Wireless Commun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

[4] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc

Volume: 05, Issue: 03, Pages:1951-1956 (2013) ISSN : 0975-0290

sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, May 2008.

[6] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Commun.Mag.*, vol. 46, no.2, pp. 112–119, Feb. 2009.

[7] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1752–1754, Oct. 2010.

[8] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp.1698–1712, Nov. 2009.

[9] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trustbased routing and intrusion detection," *IEEE Trans. Netw. Service Manag.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[10] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 2, pp. 184–197, Apr. 2012.

[11] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Netw.*, vol. 16, no. 5, pp. 1493–1510, Jul. 2010.

[12] A.Rezgui andM. Eltoweissy, " :Areliable adaptive servicedriven efficient routing protocol suite for sensor-actuator networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009.

[13] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proc. Second* IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[14] R. Ferdous, V. Muthukkumarasamy, and E. Sithirasenan, "Trust-based cluster head selection algorithm for mobile ad hoc networks," in *Proc.*2011 Int. Joint Conf. IEEE TrustCom-1111/IEEE ICESS-11/FCST-11, pp. 589–596.

[15] Z. Liang and W. Shi, "TRECON: A trust-based economic framework for efficient internet routing," *IEEE Trans. Syst., Man, Cybern. A, Syst .Humans*, vol. 40, no. 1, pp. 52–67, Jan. 2010.

[16] R. Zhou and K. Hwang, "Power-trust: A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 5, pp. 460–473, May 2007.

[17] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic frameworkof trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[18] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun.*,vol. 24, no. 2, pp. 318–328, Feb. 2006.

[19] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM Workshop Security of ad hoc and Sensor Networks (SASN'04)*, Oct. 2004, pp. 66–67.

[20] A. Boukerche, X. Li, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Commun.*, vol. 30, pp. 2413–2427, Sep. 2007.

Authors Biography

R.Satheeskumar received his B.E. and M.Tech. degree in Computer Science and Pursuing his Phd from Anna University . He is currently working as Head of the Department of Computer Science and Engineering at Bharath Engineering College , Madurai, India. His areas of interest are Data Mining, Software Engineering and Computer Networks and Wireless Sensor Networks. Currently he has published many papers in national and International journals. He is the lifetime member of ISTE and IEEE

B.Anbuselvan received his M.E. degree in Computer Science and Engineering and Pursuing his Phd from Anna University. He is currently working as Assistant Professor Department of Computer Science and Engineering at Bharath Engineering college , Madurai, India. His areas of interest are Software Testing ,Software Engineering and Computer Networks and DataStructures and Algorithms. Currently he has published many papers in national and International journals. He is the lifetime member of ISTE and IEEE.

M.kasipandi received his M.C.A degree from university department of Anna university and doing ME software Engineering from Anna University Chennai, India. His areas of interest are data mining, Software Engineering and , Wireless sensor Networks. He has presented many papers in national conference in various fields. As part of this paper, he is working on developing communication protocols for wireless networks protocols optimized for wireless sensor network. He is also investigating operating systems support for mobile hosts .He is a member of ISTE.