Middle-East Journal of Scientific Research 24 (S2): 33-39, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.S2.109

An Energy-Efficient Attack- Resistant Trust Model for Underwater Wireless Sensor Networks

C. Vennila and M. Madhura

Department of ECE, Saranathan College of Engineering, Tiruchirappalli, Tamilnadu, India

Abstract: Underwater wireless sensor network has been recently proposed to support time-critical aquatic applications such as submarine tracking and harbour monitoring. In Wireless Sensor Networks (WSNs), sensors collaborate to perform various tasks, such as routing. A trust-based scheme of routing can be used to route around compromised nodes that attempt to upset this collaboration. In the existing system, the unique characteristics of Underwater Acoustic Sensor Networks (UASN) make it impossible to directly use these trust models. In this paper, a novel Attack-Resistant Trust model based on Multidimensional trust Metrics (ARTMM) is implemented for UASNs. In the ARTMM, multidimensional trust metrics including energy levels and communication is considered.

Key words: Submarine tracking % Harbour monitoring % Compromised nodes % Trust and multidimensional metrics

INTRODUCTION

The oceans exist as the least explored frontiers on this planet and many maritime applications seem relatively slow in exploiting the state-of-the-art information-communication technologies. The shipbuilding and offshore engineering industries are also significantly interested in developing technologies such as sensor networks which is an economically viable alternative to currently existing and costly methods used in structural health monitoring, seismic monitoring, installation and mooring, etc. The underwater channel is characterized by prolonged propagation times and frequency-dependent attenuation that is highly affected by the distance between deployed nodes as well as by the link orientation. There has been a growing interest in monitoring underwater wireless mediums for scientific exploration, commercial exploitation and attack protection as it contributes for the well-being of human. Under Water Sensor Network (UWSN) consists of a variable number of sensors and vehicles that are deployed to perform collaborative monitoring tasks over a considered area. To achieve this objective, vehicles and sensors organize by their own self in an autonomous network which can adapt to the characteristics of the ocean environment. Underwater wireless sensor networks can be characterised by their spatial coverage and by the individual node density. The paper reviews the fundamentals of their physical environment and engineering implementations for efficient exchange of information via wireless communication using physical waves as the carrier among the sensor nodes in an underwater sensor network. Based on the comparative study, carriers can be selected for underwater wireless sensor networks that enhance the efficiency of communication in specified underwater environment. Underwater sensor networks are effectively utilized to enable applications for oceanographic collection of data, ocean sampling, environmental and pollution monitoring, disaster prevention, offshore exploration, tsunami and seaquake warning, assisted navigation, mine reconnaissance and distributed tactical surveillance. There is, in fact, significant interest in supervising aquatic environments for environmental, scientific, safety, commercial and military reasons. While there is a need for real-time, fine grained, highly precise spatio-temporal sampling of the ocean environment, current trending methods such as sequential local sensing and remote telemetry cannot satisfy many application needs, which makes a need for wireless underwater acoustic networking.

Corresponding Author: C. Vennila, Department of ECE, Saranathan College of Engineering, Tiruchirappalli, Tamilnadu, India.
E-mail: vennila-ece@saranathan.ac.in.

Underwater Network Deployment:

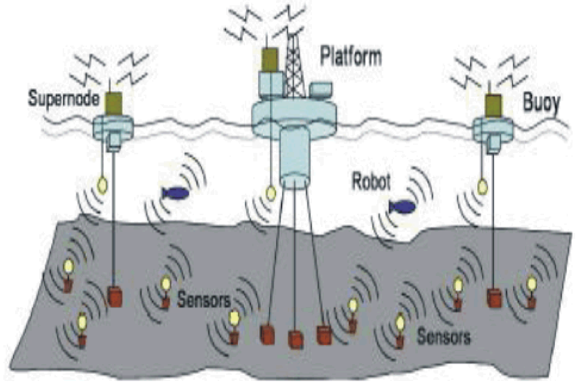

Fig. 1.1: Underwater network deployment

In Fig. 1.1, there are four different types of nodes in the system. At the lowest layer, the large number of sensor nodes are deployed on the floor of the sea (shown as small yellow circles). They collect data through attached sensors (e.g., seismic) and communicate with other neighbouring nodes through short-range acoustic modems. They operate on batteries and to operate for long periods of lifetime since they spend most of their life asleep. Many deployment strategies of these nodes are possible; here the nodes are anchored to the sea floor. There is an expectation that the nodes could be able to determine their locations through the distributed localization algorithms. At the topmost layer there are one or more control nodes with the help of connections to the Internet. The node shown on the platform in Figure 1.1 is this kind of node. These type of control nodes may be positioned on an off-shore platform, or they may be on-shore; it is expected that these nodes have a large storage capacity to buffer data and make access to ample electrical power. Control nodes will communicate directly with sensor nodes, by connecting to an underwater acoustic modem with wires.

Background and Related Work: In [1], the authors have presented an overview of the state of the art in underwater acoustic sensor network and described the challenges posed by the peculiarities of the underwater channel with particular reference to monitoring applications for the ocean environment. The ultimate objective of their work is to encourage research efforts to lay down fundamental basis for the development of new advanced communication techniques for efficient underwater communication and networking for enhanced ocean monitoring and exploration applications. In [2], the authors have proposed deployment strategies for two-dimensional and three dimensional architectures for underwater sensor networks and provided the deployment analysis. Their objectives were to determine the minimum number of sensors to be deployed to achieve the application-dependent target sensing and communication coverage; provide guidelines on how to choose the deployment surface area, given a target region; study the robustness of the sensor network to node failures and provide an estimate of the number of required redundant sensors. In [3], the authors have presented a Parameterized and Localized trUst management Scheme (*PLUS*) for sensor networks security. Compared to the existing works targeted at this field, their proposed scheme is a novel approach from whole system view to well complement current security practices. The highly abstracted parameters give the scheme flexibility to adapt to different operational environment and application domains; the localized trust model is more suitable to the less formal, temporary or short term trust relationship presented in sensor networks; the derived trustworthiness can be used to conduct efficient security actions and disclose the potential attacks. Lower computational and communication overhead are also achieved in their proposed scheme. In [4], the authors have presented a generalized and unified approach for providing data authentication by modelling it as a problem of developing a community of trustworthy sensor nodes. The authors have developed a Reputation-based Framework for Senor Networks (RFSN), where each sensor node maintains reputation for other nodes. This reputation can be used as an inherent aspect in predicting the future behaviour of the nodes, thereby allowing the identification of misbehaving nodes. RFSN integrates tools from statistics and decision theory into a comprehensive, distributed and completely scalable framework.

The authors employ a Bayesian formulation, specifically a beta reputation system, for reputation representation, updates, integration and trust evolution. Besides identifying the misbehaviour of the nodes, it is also possible to establish a relative magnitude of each node’s misbehaviour as compared to other misbehaving or good nodes. In [5], the Meandering Current Mobility model (MCM) is introduced for underwater mobile acoustic sensor networks. This is the first physically-inspired mobility model used in the analysis of mobile underwater sensor networks. The authors started an analysis of the impact that the MCM model has on the network connectivity, coverage and on the error of a range-based localization scheme. Their results show that a multiple deployment process improves the connectivity lifetime of the sensor networks by studying how the waiting time between two rounds is related to the absolute dispersion of nodes. Their mobility model is dominated by a rather complicated, vortex-driven, process of disconnection and reconnection of portions of the network. This process is common to ocean flows. The authors study how the model affects a range-based localization protocol and its impact on the coverage and connectivity of the network under different deployment scenarios. For wireless sensor networks (WSNs), many factors, such as mutual interference of wireless links, battlefield applications and nodes exposed to the environment without good physical protection, result in the sensor nodes being more vulnerable to be attacked and compromised. In order to address this network security problem, a novel trust evaluation algorithm defined as NBBTE (Node Behavioural Strategies Banding Belief Theory of the Trust Evaluation Algorithm) is proposed in [6], which integrates the approach of nodes behavioural strategies and modified evidence theory.

Trust Model Methodology: Very little work has been done in the underwater acoustic network deployment field leaving the window wide open for upcoming research and opportunities. The problems with the existing field of wireless sensor networks are as follows:

- The trust values that are calculated are inaccurate and meaningless.
- It is not reliable.
- The problem with this kind of trust estimation method is that it has a more focus on the recent behaviour of the node rather than comprehensively combining the current behaviour of the nodes with their past behaviour.
- As sensor nodes often lack tamper-resistant hardware and are easily compromised.
- This may not be always true, because an attacking node usually tries as much as possible to make detection avoidance.In this paper, the system uses a novel Attack-Resistant Trust model based on Multidimensional trust Metrics (ARTMM) for Underwater Acoustic Sensor Networks. Different from the conventional trust models, the ARTMM trust model considers the characteristics of underwater channel, e.g., low link quality, unreliable communication and mobility of sensor nodes into account. In this trust model, three types of trust metrics are considered: data trust, link trust and node trust. First, the property of inter-dependency among the three trust metrics is analysed.

Then, a concept of sliding window is adopted to calculate and dynamically update trust values of transmitted data, communication links and participating nodes. ARTMM consists of two steps: calculation of current trust in each time window and updating the trust based on historical trust values. The system adopt the ARIMA (Auto Regressive Integrated Moving Average) model to make the prediction of packet loss by minimizing the influence from noise and interference. The link trust value increased by the gradual incensement of link usage rate. The system finally obtain the trustworthiness of data through the correctness and similarity detection method. FSK improves the data rate as there is no need to wait for the channel clearing corresponding to the transmission of previous symbol on a different frequency. However, the overall efficiency of bandwidth remains low, typically much below 0.5 bits/sec/Hz due to the bandwidth expansion via frequency hopping. So in the bandwidth constrained underwater sensor networks FSK may not be suitable. Modulation can be coherent or non-coherent. For a coherent modulation tracking and channel estimation are needed if phase coherent modulation such as phase shift keying (PSK) is employed. For non-coherent DSSS, different spreading codes can be used and the receiver compares the output amplitudes from different matched filters, with each one matched to one choice of spreading codes. This avoids the use of channel estimation and tracking in underwater sensor networks. Although non-coherent modulation schemes have characteristics like high power efficiency, their low efficiency of bandwidth makes them unsuitable for high data-rate multi-user networks. Therefore, the techniques like coherent modulation have been developed for long-range, high-throughput systems.

Fig. 1.2 illustrates the architecture of ARTMM system model in which there is a list of neighbour nodes in the network on which the link quality is performed through which communication of the channel is analysed after which trust calculation and evaluation are carried out. After the generation of honest and dishonest recommendations, outlier aggregation and detection is performed. In order of making improvisation on outlier detection, all recommendations are classified into either trustworthy or untrustworthy which depends on the value of the recommendation. Each node keeps a table of neighbour nodes which stores the ID and the communication information of neighbour nodes. The network is a multi-hop network which implies that only when two sensor nodes move into each other's communication range could detect each other and start communicating.

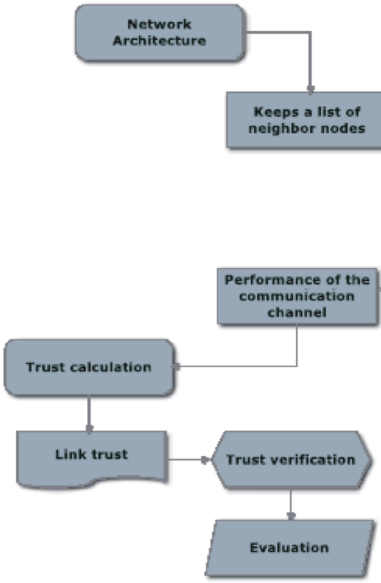

Fig. 1.2: System architecture of ARTMM model Network Architecture

The packets exchanged between any two nodes are forwarded by other forwarding nodes. At the beginning of the network deployment phase, there is an assumption that there is no malicious attack. The initial trust values of link, data and node are set to 0.5.

Link Quality Calculation: Link quality denotes the performance of the communication channel, which is evaluated based on the prediction of the packet loss and the calculation of the packet error. The actual packet loss can be predicted which is caused by the unreliable communication channel in each time window. Based on Equations, the link quality is calculated by eq. (1),

$$lq = (1\text{-}P_{per}) \times (1\text{-}P_{plr}) = (1\text{-}P_{per}) \times P_{prr} \qquad (1)$$

where,
P_{per} is the probability of packer error rate,
P_{plr} is the probability of packet loss rate and
P_{prr} is the probability of packet reception ratio.

Trust Calculation: The system use the object trust as a metric here to make evaluation of the subjective trust calculation.

Link Trust: The link trust depends on the linkcapacity and the link quality. If the link is of poor quality (lq< 0.5), even if its link capacity is very high, it is considered as untrustworthy.

Node Trust: Only direct trust can be calculated if there are large number of packets ex-changed between the nodes than the defined threshold Thnum. Otherwise, the recommendations from the common neighbour nodes are needed for object's trust evaluation. Based on this, the node trust can be defined by eq. (2) where w_{direct} and w_{recom} are the weight values of direct trust and recommendation, respectively. w_{direct} [0; 1], w_{recom} [0; 1] and $w_{direct} + w_{recom} = 1$ and S_{new} is the redefined number of successful communications:

$$T_{node} = \begin{cases} T_{direct}, \ if \ S_{new} \geq Th_{num} \\ w_{direct} \ T_{direct} + w_{recom} \ T_{recom}, \ els \end{cases} \qquad (2)$$

Data Trust: Data trust is the assessment of the fault tolerance and data consistency. It is generally known that the information of transmitted data are temporal and spatial correlation. The closer the value is to the mean, the higher the trust value is and vice-versa. Based on this idea, the data trust can be defined as in eq. (3):

$$T_{data} = 2(0.5 \ - \ \int_{m}^{vd} (x)dx) = 2\int_{vd}^{\infty} f(x)dx \qquad (3)$$

where,
$f(x)$ denotes the probability density function of data items,
µ is the mean of the data items and
x is the numerical value v_d of the data item.

Trust Verification: The method of decay principle can be implemented in many different ways. In this system, trust is calculated based on a beta probability density function, where the calculated trust values exponentially decay with time. Also, the exponential decay was used while the linear decay was used. Comparatively speaking, the exponential decay performance is better than the linear decay. Therefore, we adopt the exponential decay in the ARTMM, which is defined as in eq. (3):

$$T_{decay} = \exp\,(-* \times (t - t_0)) \qquad (3)$$

where,
* is a regulatory factor; * , (0, 1),

t is the calculation time of the current trust value and
t_0 is the calculation time of the historical trust value.

Trust Evaluation: The system compare the robustness of ARTMM, NBBTE and PTAM against underwater mobility. We adopt the movement model of the ocean water proposed in, where the velocity speed of the current flow ranges from 0m/s to 1.5m/s. In UASNs, sensor nodes collaborate with each other in order to transmit the sensed data through underwater acoustic communication channels. On the one hand, underwater sensor nodes can be attacked easily and launch many kinds of malicious attacks, e.g., data modification attack and selective forwarding attack, which produces certain amount of packet loss and the data integrity gets harmed. On the other hand, the acoustic channel is unreliable and has low link quality, which also results in a high BER and a large amount of packet loss. The performance of communication and data transmission is heavily influenced by the quality of the underwater acoustic channel. Therefore, the value of data trust is not only based on the trust of participating active sensor nodes, but also influenced by the parameter called link quality.

RESULTS AND CONCLUSION

The trust model results of the performance evaluation of the ARTMM system is compared with the existing system and the simulation is done using NS2 tool. Our technique provides higher energy than the existing one. Fig. 1.3 shows that the ARTMM is much more efficient in terms of energy than the NBBTE and the PTAM. Because in the ARTMM model, sensor nodes communicate only with their neighbour nodes. All sensor nodes only need to keep information about the neighbour nodes which implies lower energy consumption, less processing time for the calculation of trust and very less memory space. While in case of NBBTE, each node has to store the information for all the sensor nodes deployed in the network. In the PTAM model, each sensor node needs to store all the valuable information of other nodes which process the small information of the data. Therefore, the PTAM and the NBBTE consume much more energy than ARTMM.

In Fig. 1.4, the simulated malicious node attacks are selective forwarding attack (type 1), data modification attack (type 2), DoS attack (type 3), on-off attack (type 4) and bad/good mouthing attack (type 5). A parameter 'detection rate' is calculated by the number of nodes which has been detected to be malicious divided by the overall total number of malicious nodes. As shown in Fig. 1.4, it can be concluded that the performance of the ARTMM model is much better than that of the NBBTE and the PTAM. The NBBTE only considers the attack on information and the selective forwarding attack into account, thus it is vulnerable against other attacks, e.g., on-off attack, DoS attack, good/bad mouthing attack. Both the ARTMM and the NBBTE are robust against the data modification attack, but the proposed ARTMM works better. In addition, the NBBTE cannot detect malicious nodes with selective forwarding attack because in this case of simulation, the packet loss rate is assigned a constant value. The rate of data forwarding in the NBBTE is calculated based on the significant change in the number of transmission packets in different periods. The PTAM has incorporated the inter-dependency property between data and sensor nodes. Based on the data similarity check, a data modification attack can be detected. In addition, the PTAM can detect certain number of malicious nodes which launch bad/good mouthing attacks and on-off attacks. However, the terrestrial PTAM trust model is vulnerable against DoS and selective forwarding attacks. The trust value of a sensor node ranges from the value 0 to 1.

Nodes that are believed to be trustworthy have trust values close to 1 while the nodes that are considered to be untrustworthy have trust values close to 0. As mentioned, the object trust is considered as a reference to the standard global trust level that a node should be obtained by its neighbour nodes. We are using the object trust here as a metric to make an evaluation of the subjective trust calculation. First, we assume a sensor node that is considered to be completely trust without any malicious action with an object trust of 1.

The subjective trust value that is calculated should be close to 1. The more the calculated trust value is closer to 1, the more accurate it is. As shown in fig. 1.5, the robustness of ARTMM, NBBTE and PTAM against underwater mobility is compared and analysed. It can be concluded that the ARTMM can work well in underwater environment and be robust against sensor nodes' mobility, while the other two trust models which are designed without mobility consideration are not suitable for UASNs.

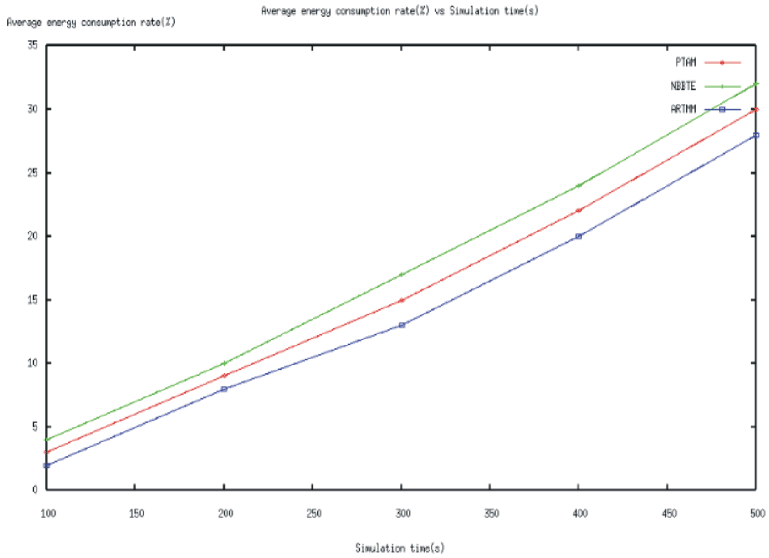

Fig. 1.3: Average energy consumption rate vs. Simulation time

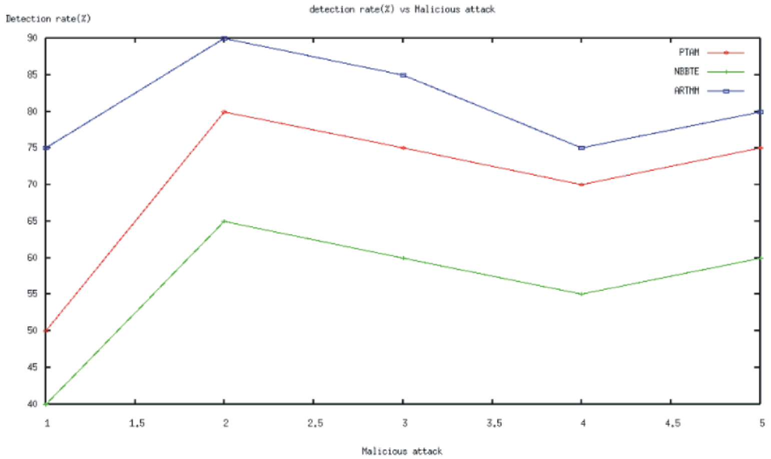

Fig. 1.4: Detection rate vs. Malicious attack

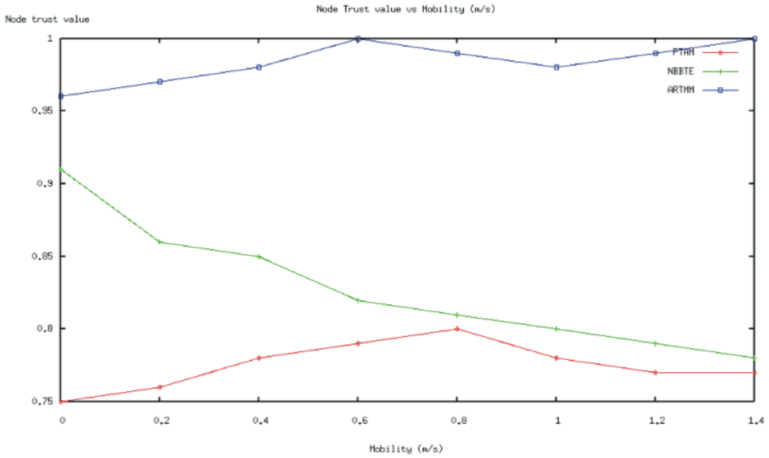

Fig. 1.5: Node trust value vs. Mobility

REFERENCES

1. Devee Prasan U. and S. Dr. Murugappan, 2012. "Underwater Sensor Networks: Architecture, Research Challenges and Potential Applications", International Journal of Engineering Research and Applications (IJERA), 2(2): 251-256.
2. Dario Pompili, Tommaso Melodia and Ian F. Akyildiz, 2006. "Deployment Analysis in Underwater Acoustic Wireless Sensor Networks", WUWNet'06, Los Angeles, California, USA, pp: 48-55.
3. Yao, Z., D. Kim and Y. Doh, 2008. "PLUS: Parameterized and Localized trust management Scheme for sensor networks security", IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp: 437-446.
4. Ganeriwal, S., L.K. Balzano and M.B. Srivastava, 2004. "Reputation-based framework for high integrity sensor networks", In Proceedings of the 2nd ACM Workshop on Security of adhoc and Sensor Networks, pp: 66-77.
5. Caruso, A., F. Paparella, L. Vieira, M. Erol and M. Gerla, 2008. "The Meandering Current Mobility Model and its Impact on Underwater Mobile Sensor Networks", INFOCOM 2008, the 27th Conference on Computer Communications, pp: 1-9, 13-18.
6. Feng, R., X. Xu, X. Zhou and J. Wan, 2011. "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory", Sensors, pp: 1345-1360.
7. Chae, Y., L. Di Pippo L.C. and Y.L. Sun, 2012. "Predictability Trust for Wireless Sensor Networks to Provide a Defense against On/Off Attack", In Proceedings of 8th International Conference on Collaborative Computing: Networking, Applications and Work sharing, Pittsburgh, PA, USA, pp: 406-405.
8. Devee Prasan, U. and S. Dr. Murugappan, 2012. "Underwater Sensor Networks: Architecture, Research Challenges and Potential Applications", International Journal of Engineering Research and Applications (IJERA), 2(2): 251-256.
9. Domingo, M.C., 2008. "Overview of channel models for underwater wireless communication networks", Physical Communication, pp: 163-182.
10. Gao, W., G. Zhang, W. Chen and Y. Li, 2009. "A Trust Model Based on Subjective Logic", The Fourth International Conference on Internet Computing for Science and Engineering, pp: 272-276.
11. He, D., C. Chen, S. Chan, J. Bu and A.V. Vasilakos, 2012. "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks". IEEE Transactions on Information Technology in Biomedicine, 16(4): 623-632.
12. Lim, H.S., Y.S. Moon and E. Bertino, 2010. "Provenance based Trust-worthiness Assessment in Sensor Networks", In Proceedings of the 7th International Workshop on Data Management for Sensor Networks, pp: 2-7.
13. Guangjie Han, Jinfang Jiang, Lei Shu and Mohsen Guizani, 2015. "An Attack-Resistant Trust Model based on Multidimensional trust Metrics in Underwater Acoustic Sensor Network", IEEE Transactions on Mobile Computing, pp: 1-14.