ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Review paper of Filtering of Attacker's Impact Using Data Aggregating Techniques in Wireless Sensor Network

Pragya Katariya[1], Prof. R.K.Krishna[2]

PG Student [CSE], Dept. of Computer Technology, Rajiv Gandhi College of Engineering,Chandrapur, Maharashtra, India[1]

Assistant Professor, Dept. of Electronics & Telecommunication, Rajiv Gandhi College of Engineering, Chandrapur, Maharashtra, India[2]

ABSTRACT: Remote Sensor Networks (WSNs) empowers the gathering of physical estimations over a huge geographic zone. Information from different sensors is collected at an aggregator hub and just the total qualities are sent to the base station .At present, impediments of the figuring force and vitality asset of sensor hubs causes information to be accumulated by to a great degree straightforward calculations, for example, averaging. Collection utilizing straightforward averaging system is exceedingly defenseless against hub trading off assaults and through the bargained sensor hubs the assailant can send false information to the aggregator to change the total qualities. Iterative separating calculations are the best answer for such reason. These calculations all the while total information from different sources and give trust estimation of these sources, for the most part in a type of relating weight variables allotted to information gave by every source. In this paper we broke down some protected information total instruments and presented another muddled intrigue assault with its effect on remote sensor systems.

KEYWORDS: Averaging method, Collusion attacks, Computing power, Data aggregation, Energy resource, Iterative filtering algorithms, Wireless sensor networks.

I.INTRODUCTION

Remote Sensor Networks are being utilized in different continuous fields like military, fiasco administration, Industry, Environmental Monitoring and Agriculture Farming and so on. Because of assorted qualities of such a variety of continuous situations, security for WSNs turns into an unpredictable issue. For every usage, there are distinctive sort of assaults conceivable and requests an alternate security level. Significant test for utilizing an effective security plan originates from the asset obliged nature of WSNs like size of sensors, Memory, Processing Power, Battery Power and so on and simple openness of remote channels by great residents and assailants.

Remote sensor systems are typically conveyed at unattended or threatening situations. In this manner, they are exceptionally helpless against different security assaults, for example, particular sending, wormholes, and Sybil assaults. What's more, remote sensor systems might likewise experience the ill effects of infusing falseinformation assault [5]. For an infusing false information assault, a foe first bargains a few sensor hubs, gets to all entering materials put away in the traded off hubs, and after that controls these bargained hubs to infuse sham data and send the false information to the sink to cause upper level error decision, as well as energy wasted in en-route nodes[12].

The Sensor Network can be portrayed as an accumulation of sensor hubs which co-ordinate to perform some particular activity. Dissimilar to conventional systems, sensor systems rely on upon thick arrangement and co-appointment to do their assignments. Sensor Networks comprised of little number of sensor hubs that were wired to a focal handling station. Nonetheless, these days, the attention is more on Wireless Sensor Networks [11].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Sensor systems are accumulation of sensor hubs which co-operatively send detected information to base station. As sensor hubs are battery driven, a productive usage of force is vital keeping in mind the end goal to utilize systems for long length of time henceforth it is expected to decrease information activity inside sensor systems, lessen measure of information that need to send to base station. The fundamental objective of information conglomeration calculations is to accumulate and total information in a vitality productive way so that system lifetime is improved. Remote sensor systems (WSN) offer an undeniably Sensor hubs require less power for preparing when contrasted with transmitting information. It is desirable over do in system preparing inside system and decrease bundle size. One such approach is information total.

Fig. 2 shows Wireless Sensor Network Architecture. Wireless sensor networks are consisting of numerous light weight and tiny sensor nodes with limited power, storage, communication and computation capabilities. Wireless sensor networks are being employed in civilian applications like habitat monitoring to mission critical Applications[20].

II. REVIEW OF DATA AGGREGRATION TECHNIQUES

This section describes the various data aggregation and data averaging techniques, network model and attack model.

2.1 Secure Data Aggregation Techniques

A few information accumulation methods have been proposed to upgrade information accessibility. Creators in [15], joins the conglomeration functionalities with the focal points gave by a notoriety framework keeping in mind the end goal to improve the system life time and the precision of the amassed information. By checking neighbourhood's exercises, every sensor hub assesses the conduct of its cell individuals keeping in mind the end goal to sift through the conflicting information in the vicinity of different traded off hubs.

Y. Sun et al. [3], achieve information reliability by broadening Josang's trust model. In light of the multilayer total construction modeling of system, they plan a trust-based structure for information collection with adaptation to non-critical failure with an objective to decrease the effect of mistaken information and give quantifiable reliability to accumulated results.

H.-S. Lim et al. [4], tended to the imperative and testing issue of guaranteeing reliability of sensor information in the vicinity of malevolent foes. They built up an amusement theoretic safeguard system to shield sensor hubs from assaults and to ensure an abnormal state of dependability for detected information. The resistance's goal technique is to guarantee that adequate sensor hubs are ensured in every assault/barrier round [6].

2.2 Network Model

The conceptual model proposed by Wagner in [25] is considered for sensor network topology. Fig. 1 shows presumption for system model in WSN. The sensor hubs are isolated into partitioned groups, and every bunch has a group head which goes about as an aggregator. Information are occasionally gathered and accumulated by the aggregator. Creators in [1] expect that the aggregator itself is not traded off and focus on calculations which make total secure when the individual sensor hubs may be bargained and may be sending false information to the aggregator. It additionally accept that every information aggregator has enough computational energy to run a suitable calculation for information total.

2.3 Data Averaging Technique

A computational productive strategy to figure a weighted normal (strong normal) of sensor estimations is proposed in [2], which appropriately takes sensor flaws and sensor commotion into thought. Creators expect that the sensors in the remote sensor system use irregular projections to pack the information and send the compacted information to the information combination focus [3]. Computational productivity of this system is accomplished by having the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

information combination focus work specifically with the packed information streams and they just needs to perform decompression once to register the vigorous normal, along these lines incredibly decreasing the computational prerequisites.

2.4 Adversary Model

The past analysts [1] [21] builds up the assault models by considering the way that they can't depend on cryptographic systems for keeping the assaults, following the enemy may extricate cryptographic keys from the bargained hubs. The creators in, considers Byzantine assault model, where the enemy can trade off an arrangement of sensor hubs and embed any false information through the bargained hubs [26]. Taking after are a few presumptions made in this model assaults in light of the fact that the foe may remove cryptographic keys from the traded off hubs [17].

c) Through the bargained sensor hubs the foe can send false information to the aggregator with a reason for changing the total qualities.

d) All bargained hubs can be under control of a solitary enemy or a conspiring gathering of foes, empowering them to dispatch a modern assault.

e) The foe has enough learning about the accumulation calculation and its parameters.

f) The base station and aggregator hubs can't be traded off by enemy hub.

III.COLLUSION ATTACK SCENARIO

In this situation ten sensors are expected that report the estimations of temperature which are collected utilizing suitable accumulation calculation Most of the calculations utilize straightforward suppositions about the beginning estimations of weights for sensors [16]. In suitable enemy display, an assailant has the capacity delude the total framework through cautious choice of reported information values. The agreement assault situations are as per the following

1) In situation 1, all sensors are reliable and the accumulation's aftereffect calculation is near the real esteem.

2) In situation 2, initial a foe bargains two sensor hubs, and modifies the readings of these qualities such that the basic normal of all sensor readings is turned towards a lower worth [22][23][24]. As these two sensor hubs report a lower quality, total calculation punishes them and allocates to them lower weights, on the grounds that theirqualities are a long way from the estimations of different sensors.

3) In situation 3, an enemy trade off three sensor hubs with a specific end goal to dispatch an intrigue assault. It listens to the reports of sensors in the system and trains the two bargained sensor hubs to report values a long way from the genuine estimation of the deliberate amount. It then processes the contorted quality [25] of the basic normal of all sensor readings and orders the third traded off sensor to report such skewed normal as its readings. At the end of the day, two traded off hubs curve the straightforward normal of readings, while the third bargained hub reports a worth near such turned normal [14].

IV.IMPACT OF COLLUSION ATTACK ON WIRELESS SENSOR NETWORK

1) In agreement assault, assailants have an abnormal state of information about the accumulation calculation and its parameters [10] henceforth they can direct convoluted assaults on remote sensor systems by infusing false information through various traded off hubs. 2) Colluders endeavor to contort the total worth by constraining accumulation calculations to meet to turned qualities gave by one of the assailants. 3) This assault is especially hazardous for remote sensor systems for two reasons [11]. a) First, trust and notoriety frameworks assume discriminating part in remote sensor systems as a strategy for determining various critical issues, for example, secure directing, adaptation to internal failure, false information recognition, bargained hub location [13], secure information total, group head race, anomaly

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

identification. b) Second, sensors which are sent in unfriendly and unattended situations [12] are very powerless against hub bargaining assaults.

This segment introduces the proposed answer for information total that can adequately moderate the effect of assaults on the WSN. The total of information is made utilizing totals like SUM, COUNT thus on with the end goal of decreasing correspondence overhead on the system [7]. The accumulation additionally can help in reducing so as to enhance effectiveness in the system general overhead on the system. In this way the proposed arrangement can profit by the total and enhances system effectiveness and backings secure correspondences also. Since the transmission and hub disappointments cause correspondence misfortunes multi-cast directing is adjusted so as to forward sub-total [8].

As appeared in Figure 4, it is apparent that the total made through the directing hubs that are a piece of WSN. The information accumulation is the hidden element of the system which guarantees that the correspondences over it are secure furthermore the effect of assaults is minimized. There are parts like base station, sensor hubs, system controller and assault examination hub. The assault examination module running in the system is mindful to sift through the information before being amassed. The assaults made on the WSN hubs will be recognized by dissecting the examples and the assault related information is sifted through at the season of conglomeration. This will conceivably lessen the effect of assaults made on the network[18][19].

Bargain hubs in the system can dispatch adulterated sub total assault with a specific end goal to hoodwink hubs and guarantee effective assaults. The distorted sub total assaults are handled by the base station as it shows a total question and with an arbitrary quality. The hubs in the system will answer the telecast question alongside MAC. In this way the base station has the capacity channel out malevolent assaults while amassing information. The potential assaults can be forestalled accordingly utilizing total method which will in the end relieve the effect of assaults made on WSN. For any piece if the substantial MAC location is not got, the base station recognizes it as pernicious and hence the effect of different assaults is lessened adequately.

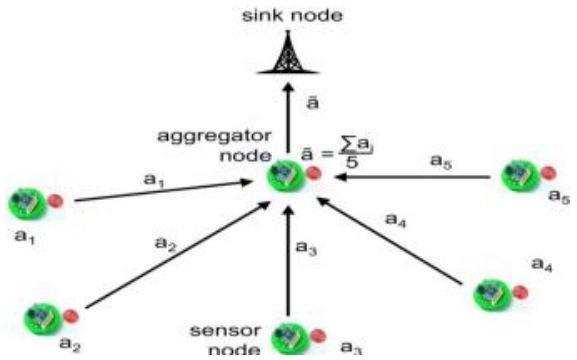

Fig1. Data Aggregation

Fig. 1 shows presumption for system model in WSN. The sensor hubs are isolated into partitioned groups, and every bunch has a group head which goes about as an aggregator.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

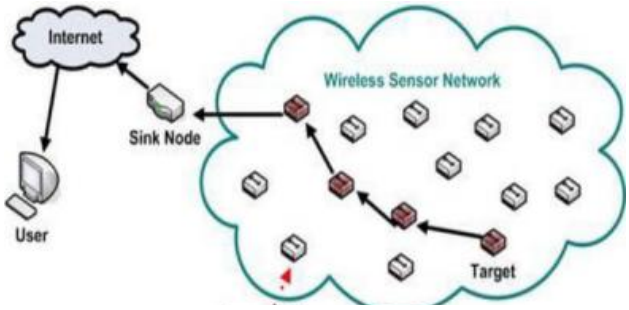

Fig 2. Wireless Network Architecture

Fig. 2 shows Wireless Sensor Network Architecture. Wireless sensor networks are consisting of numerous light weight and tiny sensor nodes with limited power, storage, communication and computation capabilities. Wireless sensor networks are being employed in civilian applications like habitat monitoring to mission critical Applications[20].

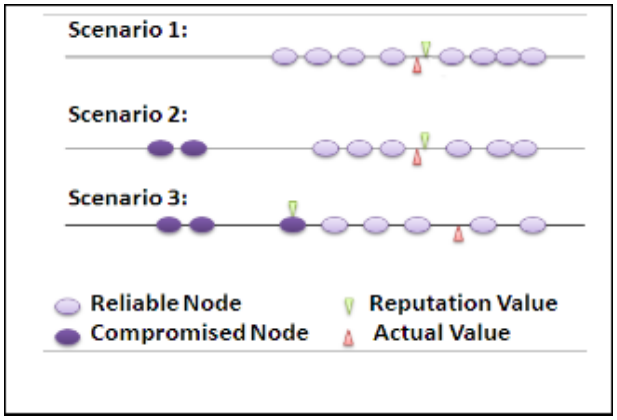

Fig 3. Collusion attack scenario

1) In situation 1, all sensors are reliable and the accumulation's aftereffect calculation is near the real esteem.

2) In situation 2, initial a foe bargains two sensor hubs, and modifies the readings of these qualities such that the basic normal of all sensor readings is turned towards a lower worth [22][23][24]. As these two sensor hubs report a lower quality, total calculation punishes them and allocates to them lower weights, on the grounds that theirqualities are a long way from the estimations of different sensors.

3) In situation 3, an enemy trade off three sensor hubs with a specific end goal to dispatch an intrigue assault. It listens to the reports of sensors in the system and trains the two bargained sensor hubs to report values a long way from the genuine estimation of the deliberate amount. It then processes the contorted quality [25] of the basic normal of all sensor readings and orders the third traded off sensor to report such skewed normal as its readings. At the end of the day, two traded off hubs curve the straightforward normal of readings, while the third bargained hub reports a worth near such turned normal [14].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

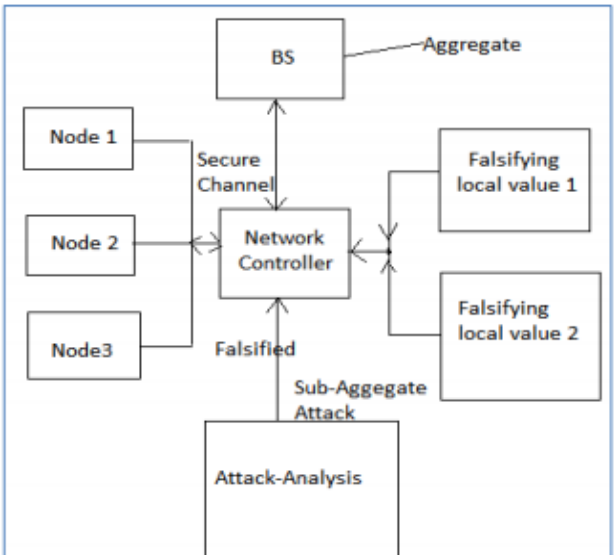

Fig4. Architectural overview of the proposed system

As appeared in Figure 4, it is apparent that the total made through the directing hubs that are a piece of WSN.

V. EXPERIMENTAL RESULTS

This area gives the earth utilized and the tests and the outcomes. The proposed framework is actualized utilizing Microsoft .NET stage. The application is the custom test system that shows the motion of a WSN [9][10]. The proposed framework is executed utilizing the structural engineering proposed as a part of the past segment. The investigations are made as far as number of traded off hubs versus deviations of the evaluation from r, number of bargained hubs versus normal per hub sent bits, and number of traded off hubs versus number of MACs.

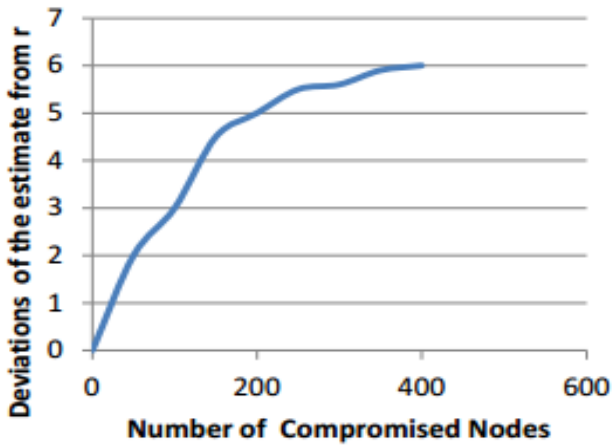

Fig. 5. Impact of number of compromised nodes

As shown in Figure 5, it is evident that the impact of the compromised node is more as the number of nodes is increased. When number of nodes is increased, the deviations of the estimate from r are more.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

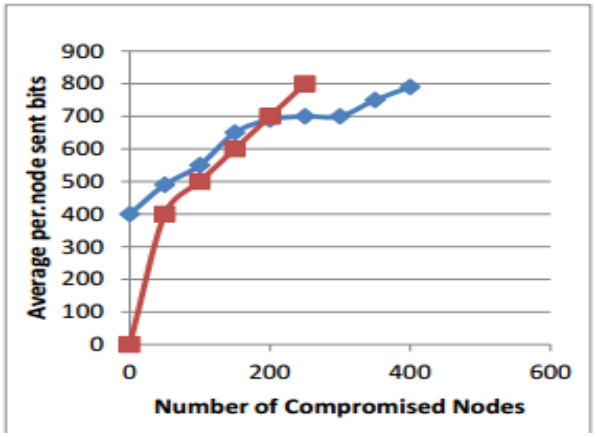

Fig. 6. Impact of number of compromised nodes

As appeared in Figure 6, it is clear that the effect of the traded off hub is more as the quantity of bargained hubs is expanded. At the point when number of hubs is expanded, the normal per hub sent bits is more.

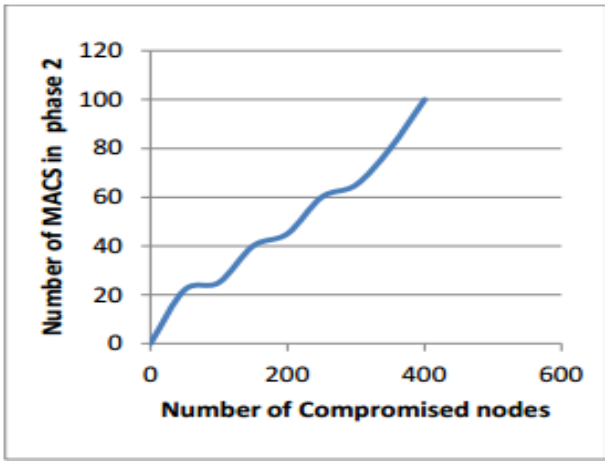

Fig.7 Impact of number of Compromised Nodes

As shown in Figure 7, it is evident that the impact of the compromised node is more as the number of compromised nodes is increased. When number of nodes is increased, the number of MACs is more.

VI.CONCLUSION

Information total components alongside information averaging methods are broke down. System model proposed by Wagner is depicted for sensor system. Enemy models with their presumptions are checked on. New advanced conspiracy assault situations alongside its effect on remote sensor systems are clarified. When computational force of low power processors altogether enhances, future aggregator hubs will be equipped for performing more troublesome information collection calculations, in this way making remote sensor arranges less defenseless. In future an improved system against arrangement assault is presented which makes is intrigue vigorous, as well as more precise and quicker uniting.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

REFERENCES

[1] Mohsen Rezvani, AleksandarIgnjatovic, Elisa Bertino, and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions on Dependable and Secure Computing (TDSC) ,2014.
[2] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults", IEEE Transactions on Parallel and Distributed Systems, August 2013.
[3] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault tolerant data aggregation in wireless multimedia sensor networks", IEEE Transaction on Dependable & Secure Computing, Nov. 2012.
[4] H. S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A game theoretic approach for high-assurance of data trustworthiness in sensor networks", IEEE International Conference on Data Engineering (ICDE), April 2012.
[5] J. W. Ho, M. Wright, and S. Das, "Zone Trust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing" IEEE Transactions on Dependable and Secure Computing, july-aug. 2012.
[6] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Journal of Network and Computer Applications, 2012.
[7] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks", IEEE Transactions on Information Forensics and Security, 2012.
[8] H. L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN", 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011.
[9] B. C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment", in Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, 2011.
[10] J. W. Ho, M. Wright, and S. K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing", IEEE Transaction on Mobile Computing, June 2011.
[11] M. Groat, W. He, and S. Forrest, "KIPDA: k-indistinguishable privacy preserving data aggregation in wireless sensor networks", in INFOCOM'2011.
[12] R. Rana, W. Hu, T. Wark, and C.T. Chou, "An Adaptive Algorithm for Compressive Approximation of Trajectory (AACAT) for Delay Tolerant Networks," Proc. Eighth European Conf. Wireless Sensor Networks, Feb. 2011.
[13] Y. Shen, W. Hu, R. Rana, and C.T. Chou, "Non-Uniform Compressive Sensing in Wireless Sensor Networks: Feasibility and Application," Proc. Seventh Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2011.
[14] V. Kumar, and S. Madria, "Secure data aggregation in wireless sensor networks," in Wireless Sensor Network Technologies for the Information Explosion Era. Springer, 2010.
[15] S. Ozdemir and H. Cam, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks", IEEE/ACM Transaction on Networking, Jun. 2010.
[16] L. A. Tang, X. Yu, S. Kim, J. Han, C.-C. Hung, and W. C. Peng, "TruAlarm: Trustworthiness analysis of sensor networks in cyberphysical systems", IEEE International Conference on Data Mining, 2010.
[17] J. Bahi, C. Guyeux, and A. Makhoul, "Efficient and robust secure aggregation of encrypted data in sensor networks," in Fourth International Conference on Sensor Technologies and Applications, July 2010.
[18] R. K. Rana, C. T. Chou, S. S. Kanhere, N. Bulusu, and W. Hu, "EarPhone: An End-to-End Participatory Urban Noise Mapping System," Proc. ACM/IEEE Ninth International Conf. Information Processing in Sensor Networks, April 2010.
[19] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in Proceedings of the 5 th International Workshop on Security and Trust Management, 2009.
[20] R. Roman, C. Fernandez Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking, 2009.
[21] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," in Proceedings of the 2009 IEEE international conference on Symposium on Information, 2009.
[22] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto, "Reputation-based Secure Data Aggregation in Wireless Sensor Networks", Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2008.
[23] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based framework for high integrity sensor networks," ACM Transaction, Jun. 2008.
[24] X. Y. Xiao, W. C. Peng, C. C. Hung, and W. C. Lee, "Using Sensor Ranks for in-network detection of faulty readings in wireless sensor networks," in Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, 2007.
[25] D. Wagner, "Resilient aggregation in sensor networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2007.
[26] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," Department of Computer Science, Johns Hopkins University, Tech. Rep., 2007.