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. 4, Issue 11, November 2016

Data Aggregation Protocol for Secure Data Transmission over Wireless Sensor Networks

Somarouthu Gani Lakshmi[1], S.V.Krishna Reddy[2]

M.Tech, Dept. of CSE, Kakinada Institute of Engineering and Technology for Women, Korangi, India[1]

Assistant Professor, Dept. of CSE, Kakinada Institute of Engineering and Technology for Women, Korangi, India [2]

ABSTRACT: Wireless Sensor Networks are used to collect the data from different devices over a large geographic area. So the collected data from devices is aggregated at a node called aggregator node and the values that are aggregated can only be forwarded to the base station. Currently there are many limitations like computation power and energy resources of sensor nodes which leads the data to be aggregated by extremely simple algorithms like averaging. But with simple averaging method, aggregation of data can be highly vulnerable and may lead to node compromising attacks; and through the compromised sensor nodes, the attacker can send false data to the aggregator to change the aggregate values. One of the most effective solutions is to use Iterative Filtering algorithms. These algorithms simultaneously aggregate data from multiple sources and provide trust estimation of sources which will be in form of corresponding weight factors assigned to data provided by each source. In this paper, various secure data aggregation mechanisms were analyzed and introduced a new complicated collusion attack with its impact on wireless sensor networks.

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

I. INTRODUCTION

Wireless Sensor Networks are being employed in various real time fields like military, disaster management, Industry, Environmental Monitoring and Agriculture Farming etc. Due to diversity of so many real time scenarios, security for WSNs becomes a complex issue. For each implementation, there are different type of attacks possible and demands a different security level. Major challenge for employing an efficient security scheme comes from the resource constrained nature of WSNs like size of sensors, Memory, Processing Power, Battery Power etc. and easy accessibility of wireless channels by good citizens and attackers.

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack [5]. For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper level error decision, as well as energy wasted in en-route nodes [12].

The Sensor Network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. Sensor Networks consisted of small number of sensor nodes that were wired to a central processing station. However, nowadays, the focus is more on Wireless Sensor Networks [11].

Sensor networks are collection of sensor nodes which co-operatively send sensed data to base station. As sensor nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration hence it is needed to reduce data traffic inside sensor networks, reduce amount of data that need to send to base station. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation.

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. 4, Issue 11, November 2016

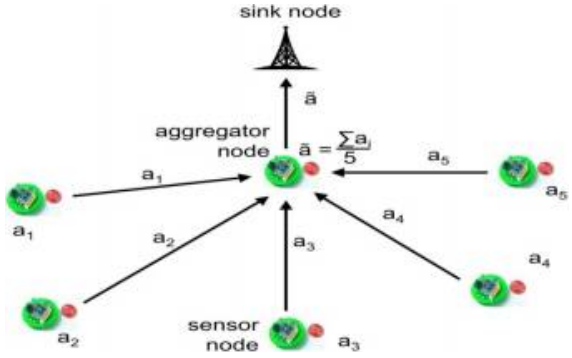

Fig.1. Data Aggregation

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].

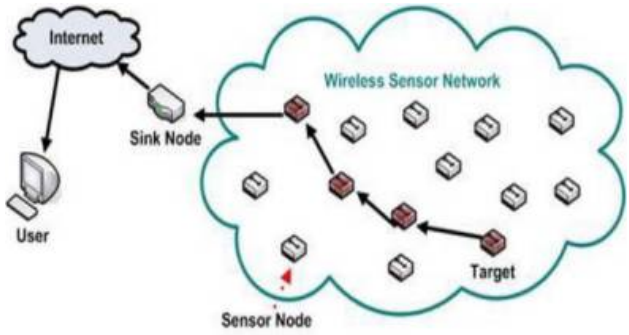

Fig. 2. Wireless Sensor Network Architecture

II. RELATED WORKS

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

A. SECURE DATA AGGREGATION TECHNIQUES

Several data aggregation techniques have been proposed to enhance data availability. Authors in [15], combines the aggregation functionalities with the advantages provided by a reputation system in order to enhance the network life time and the accuracy of the aggregated data. By monitoring neighborhood's activities, each sensor node evaluates the behaviour of its cell members in order to filter out the inconsistent data in the presence of multiple compromised nodes.
Y. Sun et al. [3], accomplish data trustworthiness by extending Josang's trust model. Based on the multilayer aggregation architecture of network, they design a trust-based framework for data aggregation with fault tolerance with a goal to reduce the impact of erroneous data and provide measurable trustworthiness for aggregated results.
H.-S. Lim et al. [4], addressed the important and challenging problem of assuring trustworthiness of sensor data in the presence of malicious adversaries. They developed a game theoretic defense strategy to protect sensor nodes from attacks and to guarantee a high level of trustworthiness for sensed data. The objective of the defense strategy is to ensure that sufficient sensor nodes are protected in each attack/defense round [6].

B. NETWORK MODEL

The conceptual model proposed by Wagner in [25] is considered for sensor network topology. Fig. 1 shows assumption for network model in WSN. The sensor nodes are divided into separate clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. Authors in [1] assume

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. 4, Issue 11, November 2016

that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator. It also assumes that each data aggregator has enough computational power to run an suitable algorithm for data aggregation.

C. DATA AVERAGING TECHNIQUE

A computational efficient method to compute a weighted average (robust average) of sensor measurements is proposed in [2], which properly takes sensor faults and sensor noise into consideration. Authors assume that the sensors in the wireless sensor network use random projections to compress the data and send the compressed data to the data fusion centre [3]. Computational efficiency of this method is achieved by having the data fusion centre work directly with the compressed data streams and they only needs to perform decompression once to compute the robust average, thus greatly reducing the computational requirements.

D. ADVERSARY MODEL

The past researchers [1] [21] develops the attack models by considering the fact that they cannot rely on cryptographic methods for preventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. The authors in, considers Byzantine attack model, where the adversary can compromise a set of sensor nodes and insert any false data through the compromised nodes [26]. Following are some assumptions made in this model

a) Sensors are deployed in a hostile unattended environment with some physically compromised nodes.

b) When a sensor node is compromised, all the information which is inside the node becomes accessible by the adversary. System cannot depend on cryptographic methods for preventing the attacks because the adversary may extract cryptographic keys from the compromised nodes [17].

c) Through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of changing the aggregate values.

d) All compromised nodes can be under control of a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack.

e) The adversary has enough knowledge about the aggregation algorithm and its parameters.

f) The base station and aggregator nodes cannot be compromised by adversary node.

III. COLLUSION ATTACK SCENARIOS

In this scenario ten sensors are assumed that report the values of temperature which are aggregated using suitable aggregation algorithm Most of the algorithms employ simple assumptions about the initial values of weights for sensors [16]. In suitable adversary model, an attacker is able to mislead the aggregation system through careful selection of reported data values. The collusion attack scenarios are as follows

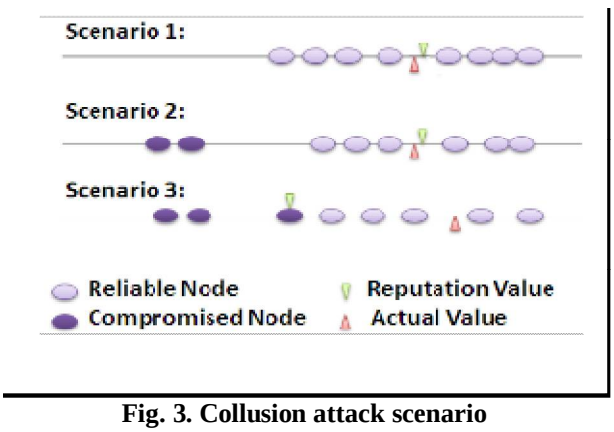

Fig. 3. Collusion attack scenario

1) In scenario 1, all sensors are trustworthy and the result of the aggregation algorithm is close to the actual value.

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. 4, Issue 11, November 2016

2) In scenario 2, first an adversary compromises two sensor nodes, and alters the readings of these values such that the simple average of all sensor readings is twisted towards a lower value [22][23][24]. As these two sensor nodes report a lower value, aggregation algorithm penalises them and assigns to them lower weights, because their values are far from the values of other sensors.

3) In scenario 3, an adversary compromise three sensor nodes in order to launch a collusion attack. It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity. It then computes the twisted value [25] of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings. In other words, two compromised nodes twist the simple average of readings, while the third compromised node reports a value very close to such twisted average [14].

A. IMPACT OF COLLUSION ATTACK ON WIRELESS SENSOR NETWORK

1) In collusion attack, attackers have a high level of knowledge about the aggregation algorithm and its parameters [10] hence they can conduct complicated attacks on wireless sensor networks by injecting false data through a number of compromised nodes. 2) Colluders attempt to twist the aggregate value by forcing aggregation algorithms to converge to twisted values provided by one of the attackers. 3) This attack is particularly dangerous for wireless sensor networks for two reasons [11]. a) First, trust and reputation systems play critical role in wireless sensor networks as a method of resolving a number of important problems, such as secure routing, fault tolerance, false data detection, compromised node detection [13], secure data aggregation, cluster head election, outlier detection. b) Second, sensors which are deployed in hostile and unattended environments [12] are highly vulnerable to node compromising attacks.

IV. PROPOSED SOLUTION

This section presents the proposed solution for data aggregation that can effectively mitigate the impact of attacks on the WSN. The aggregation of data is made using aggregates like SUM, COUNT and so on for the purpose of reducing communication overhead on the network [7]. The aggregation also can help in improving efficiency in the network by reducing overall overhead on the network. Thus the proposed solution can benefit from the aggregation and improves network efficiency and supports secure communications as well. Since the transmission and node failures cause communication losses multi-cast routing is adapted in order to forward sub-aggregate [8].

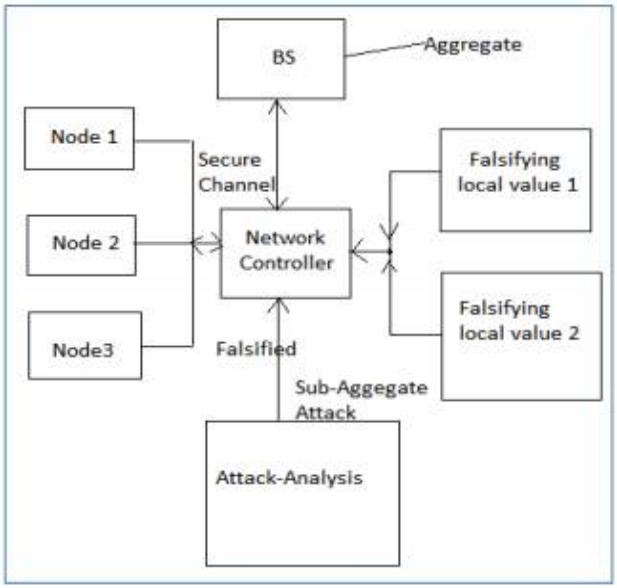

Fig. 4. Architectural Overview of the Proposed System

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. 4, Issue 11, November 2016

As shown in Figure 2, it is evident that the aggregation made through the routing nodes that are part of WSN. The data aggregation is the underlying feature of the network which ensures that the communications over it are secure and also the impact of attacks is minimized. There are components like base station, sensor nodes, network controller and attack-analysis node. The attack analysis module running in the network is responsible to filter out the data before being aggregated. The attacks made on the WSN nodes will be identified by analyzing the patterns and the attack related data is filtered out at the time of aggregation. This will potentially reduce the impact of attacks made on the network[18][19].

Compromise nodes in the network can launch falsified sub aggregate attack in order to deceive nodes and ensure successful attacks. The falsified sub aggregate attacks are tackled by the base station as it broadcasts an aggregate query and with a random value. The nodes in the network will answer the broad cast query along with MAC. Thus the base station is able to filter out malicious attacks while aggregating data. The potential attacks can be prevented thus using aggregation technique which will eventually mitigate the impact of attacks made on WSN. For any bit if the valid MAC address is not received, the base station identifies it as malicious and thus the impact of various attacks is reduced effectively.

V. EXPERIMENTAL RESULTS

This section provides the environment used and the experiments and the results. The proposed system is implemented using Microsoft .NET platform. The application is the custom simulator that demonstrates the dynamics of a WSN [9][10]. The proposed system is implemented using the architecture proposed in the previous section. The experiments are made in terms of number of compromised nodes vs. deviations of the estimate from r, number of compromised nodes vs. average per node sent bits, and number of compromised nodes vs. number of MACs.

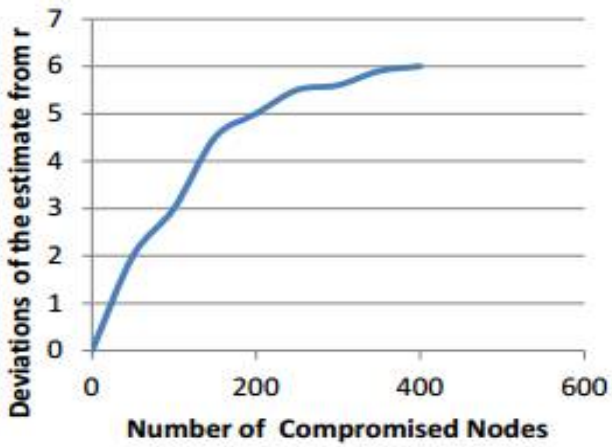

Fig. 5. Impact of number of compromised nodes

As shown in Figure 3, 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. 4, Issue 11, November 2016

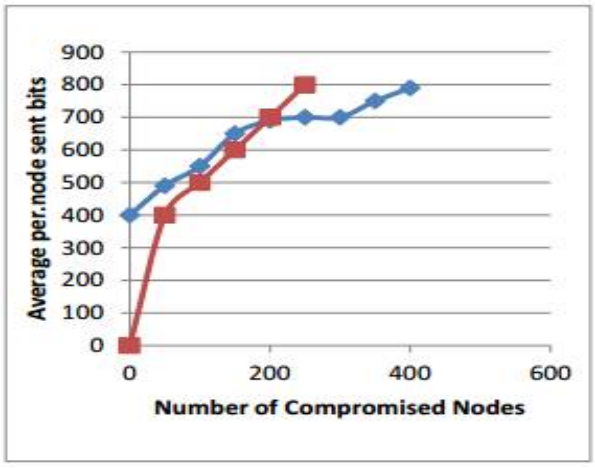

Fig. 6. Impact of number of compromised nodes

As shown in Figure 4, 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 average per node sent bits is more.

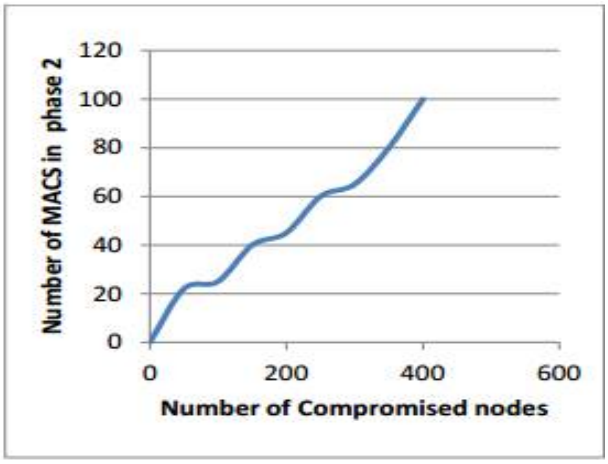

Fig. 7. Impact of number of compromised nodes

As shown in Figure 5, it is evident that the impact of the compromised node is more as the number of compromised nodes is increased. When number of nodes is increased, the number of MACs is more.

IV. CONCLUSION

Data aggregation mechanisms along with data averaging techniques are analysed. Network model proposed by Wagner is described for sensor network. Adversary models with their assumptions are reviewed. New sophisticated collusion attack scenarios along with its impact on wireless sensor networks are explained. As soon as computational power of very low power processors significantly improves, future aggregator nodes will be capable of performing more difficult data aggregation algorithms, thus making wireless sensor networks less vulnerable. In future an enhanced strategy against collusion attack is introduced which makes is not only collusion robust, but also more accurate and faster converging

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. 4, Issue 11, November 2016

REFERENCES

[1] Mohsen Rezvani, Aleksandar Ignjatovic, 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.

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. 4, Issue 11, November 2016

BIOGRAPHY

Ms.somarouthu gani lakshmi: is Pursing M.Tech in computer science and Engineering from Kakinada inst of engg and technology for women, korangi. And completed Btech from Adarsh College of engg in 2014, chebrolu.

S.V.Krishna Reddy: Presently Working As Assistant Professor In Computer Science And Engineering, Kakinada Institute Of Engineering And Technology For Women,Korangi 5 Years Experince, DBMS, Datamining M. Tech Aditya Engineering College Surampalem