Implementation of Data Aggregation and Authentication in Wireless Sensor Networks

S. Chaitanya Rami Reddy, P. Ravinder Kumar

Abstract— ***Wireless sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery and eavesdropping. Sensor nodes can be compromised by intruders and the compromised nodes can distort data integrity by injecting false data. The transmission of false data depletes the constrained battery power and degrades the bandwidth utilization [1]. False data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. In this paper it has been assumed that some sensor nodes are selected dynamically as data aggregators and the nodes between two consecutive data aggregators are called forwarding nodes simply because they forward data. To detect false data injected by a data aggregator while performing data aggregation, some neighbouring nodes of the data aggregator (called monitoring nodes) also perform data aggregation and compute MACs for the aggregated data to enable their pair mates to verify the data later. This project presents a Data Aggregation and Authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates. This project introduces a data aggregation and authentication protocol (DAA) to provide false data detection and secure data aggregation against up to T compromised sensor nodes, for T>=1. The value of T depends on security requirements, node density, packet size and the amount of tolerable overhead. Microsoft C#.NET programming language is used to implement the Data aggregation and authentication protocol. The front end of the protocol is designed using Visual Studio2005.***

Index Terms— ***Authentication, Data aggregation, Data integrity, Network- level security, Sensor networks.***

I. INTRODUCTION

As the technology are improving, the demands of end users and their applications increasing. A wide variety of new applications are being invented daily. These applications have different demands from the underlying network protocol suite. High bandwidth internet connectivity has become a basic requirement to the success of almost all of these areas. Wireless Local Area Networks (WLANs) has become one of the most promising and successful technology in recent years. WLANs provide free wireless connectivity to end users, offering an easy and viable access to the network and its services. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink).

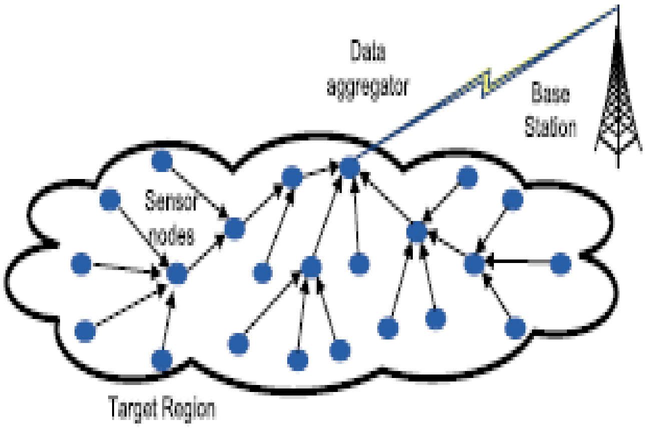


Fig. 1 Data aggregation in a wireless sensor network

In the rest of the paper, the term data aggregation is used to denote the process of data gathering with aggregation. This technique is used to avoid the implosion and overlaying problems in WSN's.

Due to the low deployment cost requirement of wireless sensor networks, sensor nodes have simple hardware and severe resource constraints. Hence, it is a challenging task to provide efficient solutions to data gathering problem. Among these constraints, "battery power" is the most limiting factor in designing wireless sensor network protocols. Therefore, in order to reduce the power consumption of wireless sensor networks, several mechanisms are proposed such as radio scheduling, control packet elimination, topology control, and most importantly data aggregation. Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced. An example for data aggregation scheme is presented in Fig 1, where a group of sensor nodes collect information from a target region [7].

It is a challenging task to protect sensitive information transmitted by wireless sensor networks. In addition, wireless sensor networks have security problems that traditional networks do not face. Therefore, security is an important issue for wireless sensor networks and there are many security considerations that should be investigated. In this section, we present the essential security requirements that are raised in a wireless sensor network environment and explain how these requirements relate with data aggregation process. Fig.2 illustrates the interaction between wireless sensor network security requirements and data aggregation process.

A. Data Confidentiality

In wireless sensor networks, data confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized parties and it is the most important issue in mission critical applications.

Manuscript Received on November, 2012.

Mr. S.Chaitanya Rami Reddy, Dept of ECE, JNT University/ JPNCE/Mahabubnagar,India.

Mr. P.Ravinder Kumar, Dept of ECE,JNT University/ JPNCE,Mahabubnagar,India.

A sensor node should not leak its readings to neighboring nodes. Moreover, in many applications, sensor nodes transmit highly sensitive data, e.g., secret keys; and therefore it is extremely important to build secure channels among sensor nodes.

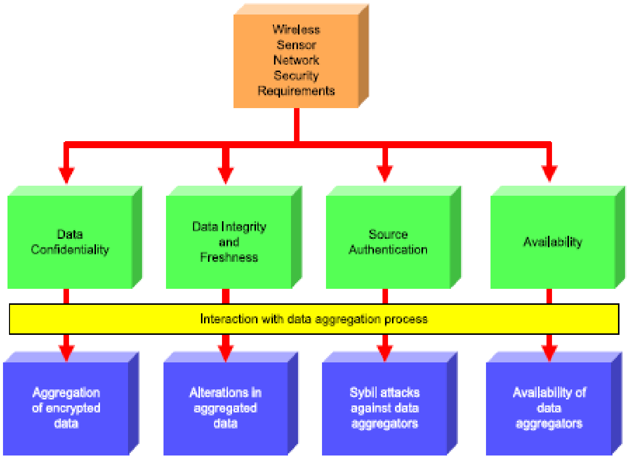

Wireless Sensor Network Security Requirements
Data Confidentiality
Data Integrity and Freshness
Source Authentication
Availability
Interaction with data aggregation process
Aggregation of encrypted data
Alterations in aggregated data
Sybil attacks against data aggregators
Availability of data aggregators

Fig. 2 Interaction between wireless sensor network security and data aggregation process

Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Furthermore, routing information must also remain confidential in certain cases as malicious nodes can use this information to degrade the network‟s performance. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.

B. Data Integrity

Data confidentiality guarantees that only intended parties obtain the un-encrypted plain data, it does not protect data from being altered. Data integrity guarantees that a message being transferred is never corrupted. A malicious node may just corrupt messages to prevent network from functioning properly. In fact, due to unreliable communication channels, data may be altered without the presence of an intruder. Thus, message authentication codes or cyclic codes are used to prevent data integrity. Data aggregation results in alterations of data.

C. Source Authentication

Wireless sensor networks use a shared wireless medium, sensor nodes need authentication mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without source authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to data aggregation protocols. If only two nodes are communicating, authentication can be provided by symmetric key cryptography. The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data.

D. Secure Data Aggregation

Like any other wireless sensor network protocol, data aggregation protocols must satisfy the security requirements [7-8]. However, the resource constrained sensor nodes and necessity of plain data for aggregation process pose great challenges when implementing security and data aggregation together. Security requirements of wireless sensor networks can be satisfied using either symmetric key or asymmetric key cryptography. Due to resource constraints of sensor nodes, symmetric key cryptography is preferable over asymmetric key cryptography. Hence, the necessity of implementing data aggregation and security using symmetric key cryptography algorithms have led many researchers to work on secure data aggregation problem. In these protocols, security and data aggregation are achieved together in a hop-by-hop fashion. That is, data aggregators must decrypt every message they receive, aggregate the messages according to the corresponding aggregation function, and encrypt the aggregation result before forwarding it.

II. OBJECTIVES OF THE SYSTEM

The main objectives of this protocol are:

- To present a novel based security protocol called data aggregation and authentication protocol (DAA), to integrate false data detection with data aggregation and confidentiality.
- To reduce the amount of transmitted data over the wireless sensor network with the help of data aggregation and early detection of false data, to a significant improvement in bandwidth utilization and energy consumption.
- To provide secure data transmission.
- To avoid Implosion and Overlaying problems in Wireless Local Area Networks.

III. RELATED WORK

To detect false data injections, presently available existing systems that employ multiple MACs are

i) Statistical en-route detection scheme.

ii) Interleaved hop-by-hop authentication against false data injection attacks in sensor networks.

iii) Commutative cipher based en-route filtering in wireless sensor networks.

iv) A dynamic en-route scheme for filtering false data in wireless sensor networks.

In statistical en-route detection scheme, called SEF, enables relaying nodes and base station to detect false data with a certain probability. In 10 hops, SEF is able to drop 80%–90% of the injected false reports [2].

In the interleaved hop-by-hop authentication scheme, any packet containing false data injected by T compromised sensor nodes is detected by those T+1 sensor nodes that collaborate to verify data integrity. In the interleaved hop-by-hop authentication scheme, sensor nodes are not allowed to perform data aggregation during data forwarding [3].

The Commutative Cipher based En-route Filtering scheme (CCEF) drops false data en-route without symmetric key sharing. In CCEF, the source node establishes a secret association with base station on a per-session basis, while the intermediate forwarding nodes are equipped with a witness key. With the use of a commutative cipher, a forwarding node can use the witness key to verify the authenticity of the reports without knowing the original session key [4].

In the dynamic en-route filtering scheme, false data are filtered in a probabilistic nature in the sense that a forwarding node can validate the authenticity of a report only if it has a corresponding authentication key. A legitimate report is endorsed by multiple sensor nodes using their distinct authentication keys from one-way hash chains [6].

The existing false data detection algorithms address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. For instance, the basic idea behind the false data detection algorithm is to form pairs of sensor nodes such that one pair-mate computes a message authentication code (MAC) of forwarded data and the other pair-mate later verifies the data using the MAC.

IV. PROPOSED SYSTEM

The proposed system presents a data aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates. This paper introduces a data aggregation and authentication protocol (DAA) to provide false data detection and secure data aggregation against up to T compromised sensor nodes, for T>=1. The value of T depends on security requirements, node density, packet size, and the amount of tolerable overhead. It is assumed that some sensor nodes are selected dynamically as data aggregators, and the nodes between two consecutive data aggregators are called forwarding nodes simply because they forward data.

In the proposed system to support confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. It also avoids the implosion and overlaying problems in WSN's.

V. DATA AGGREGATION AND AUTHENTICATION PROTOCOL

Input: A wireless sensor network with densely deployed sensor nodes [1], some of which are designated as data aggregator for a given value of T, data aggregator are already selected in such a way that,

i) There exist at least T nodes between any two data aggregators

ii) Each data aggregator has at least T neighboring nodes.

Output: Even though the network can have up to T compromised nodes, data are aggregated in data aggregators; data confidentiality is provided and the injected false data are detected and dropped.

Step1: Neighboring nodes of each data aggregator and randomly selected as monitoring nodes to perform additional data aggregation and to compute sub WSN's of the aggregated data.

Step2: The following 2T+1 pair of nodes are formed by enabling the nodes of every pair to share a distinct symmetric key:

- ❖ One pair is formed by the current and forward data aggregator.
- ❖ T pairs are formed by the monitoring nodes of the current data aggregator and the neighboring nodes of the forward data aggregator.
- ❖ T pairs are formed by the monitoring and forwarding nodes of the current data aggregator. If two nodes wants to form a pair but do not have shared key they are assumed to establish a pair-wise shared key using an existing key establishment algorithms.

Step3: Each data aggregator and its selected T monitoring nodes aggregate data and then compute subMAC's. The aggregated data are encrypted by the current data aggregator. The data aggregator and its monitoring nodes compute two subMAC‟s: One subMAC for encrypted aggregated data and another subMAC for plain aggregated data. The current data aggregator constructs two FMAC‟s from these subMAC‟s and sends the encrypted data is verified by forwarding pairmates of the selected monitoring nodes of the current data aggregator. The integrity of the plain data is verified by the some neighboring nodes of the forward data aggregator. If the integrity verification of the encrypted or plain data fails at any sensor node the data are dropped immediately.

VI. SYSTEM DESIGN

Fig. 3 shows the functional block diagram of the proposed system. It contains the following modules

1. Networking Module
2. Stream Module
3. Message authentication codes Module
4. Key recovery Module
5. Authentication Module

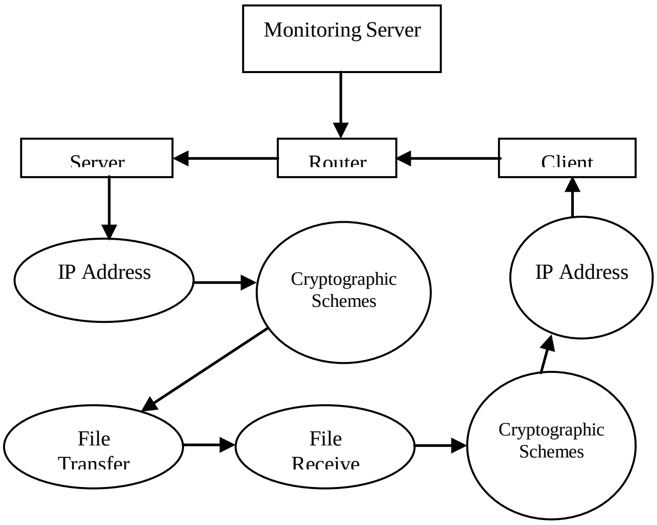


Fig. 3 Block diagram of the system

A. Networking Module

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients.

Often clients and servers operate over a computer network on separate hardware.

A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates.

B. Streaming Module

A stream cipher is a symmetric encryptor (i.e., the transmitter and receiver share the same secret key). The key forms a seed which generates a pseudorandom key-stream. At the transmitting end, this key stream is XOR-ed with the clear text stream, yielding a cipher text stream. The receiver, having the same seed key, generates synchronously the same key-stream. XOR-ing with the received cipher text yields the clear text back. Stream ciphers operate at a higher speed than block ciphers and have relatively low hardware complexity.

C. Message Authentication Codes Module

A short section of the output is stored, without entering a long key-stream into a CRC circuitry; the one-way feature of the transformation is still kept. However, a relatively short string does not exhibit randomness properties and rather represents a limited event that may have a problematic pattern. Therefore, generating a relatively long key-stream and entering it into a CRC circuitry, which preserves the randomness of its input, is desired.

D. Key Recovery Module

Recovering S from a compressed version of the cipher's output key-stream, even if the compression is based on a simple linear CRC, cannot have a lower complexity than the recovery of S from a fully given key-stream. As the latter is expected to be infeasible for secure cipher, the irreversibility of the transformation is at least as strong as the underlying security of the cipher.

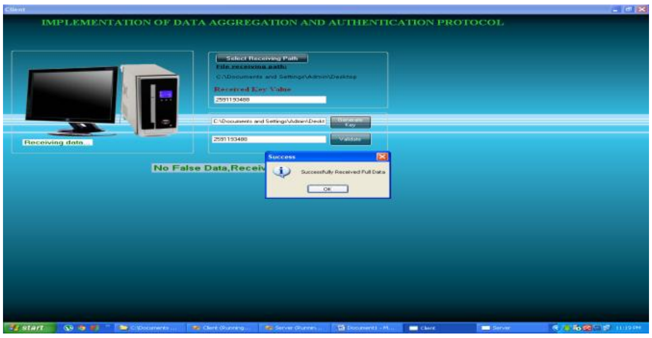
E. Data Aggregation and Authentication Module

MAC (M K) is a one-way transformation of the message M and a secret key K. The implementation this transformation can be based on various approaches. Hash Message Authentication Code (HMAC) is a hash transformation parameterized with a secret key. That is, it is an implementation of MAC (M K). In this paper, we treat a standardized HMAC, The security of such implementations has been revised, stating that the attacks "do not contradict the security proof of HMAC, but they improve our understanding of the security of HMAC based on the existing cryptographic hash functions.

VII. RESULTS AND DISCUSSIONS

In this section the simulation results of the Data aggregation and authentication protocol are discussed. The software for DAA protocol is simulated using VB2005 and the coding language used to implement software program is C#.NET. Simulation results are taken with respect to false data detection and data aggregation. For demonstration we have considered the transmission of the file to same Destination IP address two times. In first case it results in successful transmission of data as shown in Fig.4.

In Fig.4, we observed that No False data is injected and received successfully. Fig.5 shows the graph of Average Received Data and Key Value. It clearly shows both the Key Values are same. Therefore No False Data is injected into the transmitted File.



IMPLEMENTATION OF DATA AGGREGATION AND AUTHENTICATION PROTOCOL

File receiving path:
C:\Documents and Settings\Admin\Desktop

Received Key Value
2591193488

C:\Documents and Settings\Admin\Deskt
2591193488

Receiving data...

No False Data,Receiv

Success
Successfully Received Full Data

Fig.4 Snapshot of Client home window showing Successfully Received Full Data

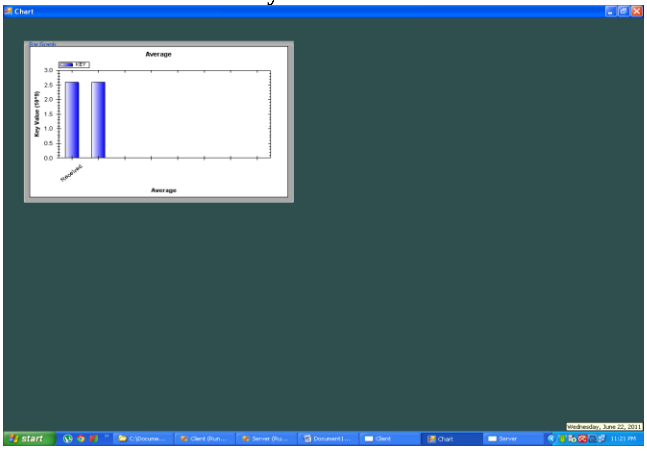
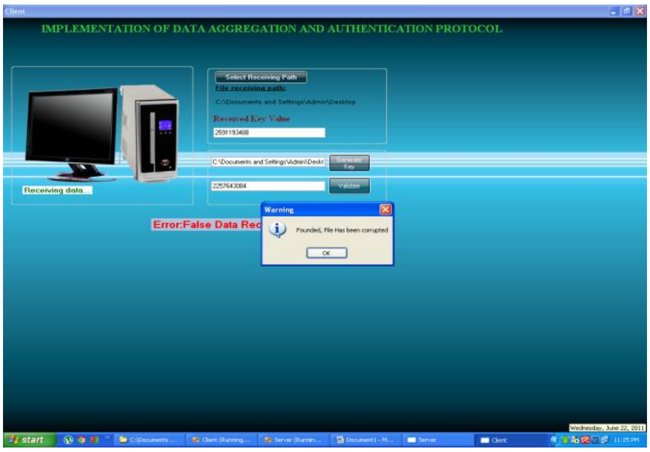


Fig.5 Graph of Average Received Data v/s Key Value.

In second case we considered transmission of the same file to the same Destination IP address. In this case since Client already received a copy of the file while aggregating the data a teach sensor node proposed protocol comes to know this file is already existing in the destination IP address.



IMPLEMENTATION OF DATA AGGREGATION AND AUTHENTICATION PROTOCOL

File receiving path:
C:\Documents and Settings\Admin\Desktop

Received Key Value
2591193488

C:\Documents and Settings\Admin\Deskt
2257643084

Receiving data...

Error:False Data Rec

Warning
Founded, File Has been corrupted

Fig.6 Snapshot of Client home window showing detection of Corrupted File

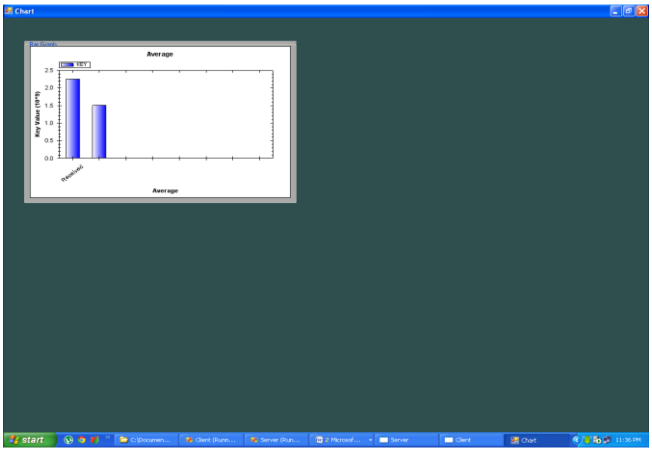


Fig.7 Graph of Average Received Data v/s Key Value

So it detects this file as corrupted file and ignores the file as shown in Fig.6. Also it avoids the reception of the files with same names. So the proposed protocol is used to avoid the implosion and overlaying problems in WSN’s. Fig.7 shows the graph of Average Received Data and Key Value. It clearly shows both the Key Values are different. Therefore it drops the corrupted file. Therefore the reception of multiple copies of the same file is avoided due to data aggregation. Finally we can conclude that Data aggregation and authentication protocol integrates data aggregation, confidentiality and false data detection. It also reduces the amount of data transmitted over the Wireless sensor network with the help of data aggregation and early detection of false data.

VIII. CONCLUSION AND FUTURE WORK

In this section, summary, conclusion, and future scope are discussed. The proposed protocol detects any false data injection it also provides data confidentiality. To provide data confidentiality during data forwarding between every two consecutive data aggregators, the aggregated data are encrypted at data aggregators, and false data detection is performed over the encrypted data rather than the plain data. Whenever the verification of encrypted data fails at a forwarding node, the data are dropped immediately to minimize the waste of resources such as bandwidth and battery power due to false data injection. It also provides false data detection and secure data aggregation against up to T compromised sensor nodes, for T>=1. The value of T depends on security requirements, node density, packet size and the amount of tolerable overhead. For the future work, we consider enabling of every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency.

REFERENCES

1. Suat Ozdemir and Hasan Çam, Senior Member, “Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks”, IEEE/ACM Trans. on networking, Vol. 18, No. 3, June 2010.
2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, IEEE Commun. Mag., Vol. 40, No. 8, pp. 102–114, Aug 2002.
3. F. Ye, H. Luo, S. Lu and L. Zhang, “Statistical en-route detection and filtering of injected false data in sensor networks”, in Proc. IEEE INFOCOM, Vol. 4, pp. 2446– 2457, 2004.
4. S. Zhu, S. Setia, S. Jajodia and P. Ning, “Interleaved hop-by-hop authentication against false data injection attacks insensor networks”, ACM Trans. Sensor Netw., Vol. 3, No. 3, Aug 2007.
5. H. Yang and S. Lu, “Commutative cipher based en-route filtering in wireless sensor networks”, in Proc. IEEE VTC, Vol. 2, pp. 1223–1227, 2004.
6. Z. Yu and Y. Guan, “A dynamic en-route scheme for filtering false data in wireless sensor networks”, in Proc. IEEE INFOCOM, pp.1 12, Apr 23–27, 2006.
7. L. Hu and D. Evans, “Secure aggregation for wireless networks”, in Proc. Workshop Security Assurance Ad hoc Netw., pp. 384–394, Jan.28, 2003,.
8. B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks”, pp. 255–265, in Proc. SenSys, 2003.

AUTHORS PROFILE

Mr. S.Chaitanya Rami Reddy, obtained my B.Tech from Kuppam Engineering Collage affiliated to JNTU Hyderabad, Chittoor District, Andhra Pradesh, India in 2008. Now I am Pursing M.Tech from Jaya Prakash Narayan College of Engineering,Mahabubnagar affiliated to JNTU Hyderabad,Andhra Pradesh,India. I participated in national seminars and I am interested in wireless networks and signal processing.

Mr. P.Ravinder Kumar, M.Tech (WMC) from Vardhaman College of Engineering,B.Tech(ECE) from Jaya Prakash Narayan College of Engineering. Currently he is working as Associate Professor at JayaPrakash Narayana College of Engineering and has 9 years of experience in teaching.I have interests in computer networks and communications,wireless networks,signal processing.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication