Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme

S. Sajithabanu,
Assistant Professor
Department of MCA
Mohamed Sadak Engineering College
Kilakarai, Tamilnadu, India.

M. Durairaj , PhD
Assistant Professor
Department of Computer Science
Bharathidasan University
Trichy, Tamilnadu, India.

ABSTRACT
Wireless sensor networks (WSNs), as an emerging technology face numerous challenges. Sensor nodes are usually resource constrained and also vulnerable to physical attacks or node compromises. As the projected applications for wireless sensor networks range from smart applications such as traffic monitoring to critical military applications such as measuring levels of gas concentration in battle fields, security in sensor networks becomes a prime concern. In sensitive applications, it becomes imperative to continuously monitor the transient state of the system rather than steady state observations and take requisite preventive and corrective actions. Generally, the networks are prone to be attacked by adversaries who intend to disrupt the functioning of the system by compromising the sensor nodes and injecting false data into the network. So it is important to shield the sensor network from false data injection attacks. In this work, it is proposed to use a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data based on Bloom Filter.

Keywords
Wireless Sensor Networks, Bandwidth, Injecting false data attack, Bloom Filter.

1. INTRODUCTION
Wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components [1].

Wireless sensor network is a collection of nodes organized into a cooperative network [2]. Each node consists of processing capability with one or more microcontrollers, CPUs or DSP chips and may contain multiple types of memory or flash memory which holds program or data. Each node has a RF transceiver usually with a single Omni- directional antenna, and a power source such as batteries and solar cells, and accommodates various sensors and actuators.

The advancements in micro electronics and wireless communications have led to the creation of the wireless sensor network (WSN) technology. This technology has many applications including various environmental monitoring. A primitive objective of WSNs is to answer queries by gathering sensory data from the deployed sensors. The process of

collecting sensory data is generally called as 'in-network processing' or 'aggregation'. Since sensor nodes in WSN technology are usually tiny micro-electronic devices which have limited resources like low processor speed, small memory size, low computation and communication power, it becomes very challenging to design mechanisms to support data queries.

1.1 Wireless Sensor Networks
Wireless sensor network (WSN) is an emerging technology that has resulted in a variety of applications. Many applications such as health care, medical diagnostics, disaster management, military surveillance and emergency response have been deploying such networks as their main monitoring framework [2]. Basically, a wireless sensor network consists of a number of tiny sensor nodes connected together through wireless links. Some more powerful nodes may operate as control nodes called base stations. Often, the sensing nodes are referred to as 'motes' while base stations are sometimes called 'sinks'. Each sensor node can sense data such as temperature, humidity, pressure from its surroundings, conduct simple computations on the collected data and send it to other neighboring nodes through the communication links. Control nodes may further process the data and probably transfer it to a database server via a wired connection. Figure 1 shows a typical architecture for a WSN. The sensing nodes known as 'motes' are represented by black spheres and are responsible for observing the surrounding environment whereas the cube represents a control node known as 'sink' which serves as the base station.

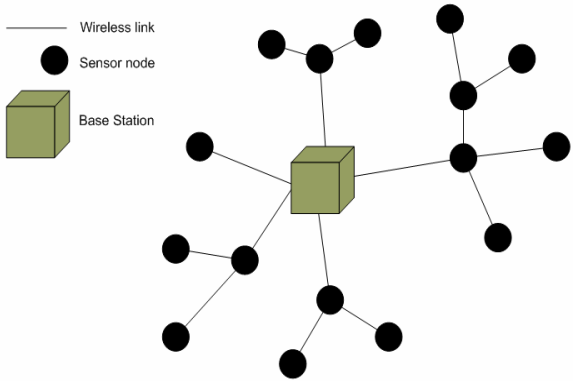

Fig 1: Typical WSN Architecture

2. SYSTEM MODELS AND ASSUMPTIONS

2.1 Sensor Network Model

In this work, it is considered that a sensor network is composed of a large number of small sensor nodes. Further it is assumed that the sensor nodes are deployed in high density so that a stimulus (e.g., a tank) can be detected by multiple sensors. Each of the detecting sensors reports its sensed signal density and one of them is elected as the center-of-stimulus (CoS) node.The CoS collects and summarizes all the received detection results, and produces a synthesized report on behalf of the group. The report is then forwarded towards the sink, potentially traversing a large number of hops (e.g., tens or more). The sink is a data collection center with sufficient computation and storage capabilities and it may also implement advanced security solutions to protect itself.

Due to cost constraints, it is assumed that each sensor node is not equipped with tamper-resistant hardware. However, dense deployment of sensor nodes enables cross-verification of a reported event among multiple sensors even in the presence of one or more compromised nodes. Statistical en-route filtering (SEF) design is not favouring the advantage of large-scale deployment [8]. SEF uses more number of small sensors than relying on a small number of powerful and expensive sensors for reliable sensing and reporting.

2.2 Threat Model

The assumption is that the attacker may know the basic approaches of the deployed security mechanisms by either compromising a node through the radio communication channel or physically capturing a node to get the security information. However, it is assumed that attackers cannot subvert the data collection unit since the sink is protected in order to defeat such subversion efforts. A node can be used to inject false reports into the sensor network once it is compromised. Naive impersonation of a sensor node can be prevented by the node and message authentication mechanisms [4]-[6]. These node and message authentication mechanisms cannot block compromised nodes from false injection of sensing reports.

A compromised sensor node can launch various other attacks besides its false data injection. It can stall the generation of reports for real events and false negative attacks. It can also stall record and replay of old reports. This paper focuses on the detection of false positive attacks or false event reports injected by compromised nodes. The main objective is to tackle threats from the compromised components. In this work, it is planned to address other attacks in subsequent efforts.

3. EXISTING SYSTEM

Once a node is compromised it is difficult to identify the node since most of the filtering mechanisms use the symmetric key technique. Usually, wireless sensor networks are deployed at unattended or hostile environments. Therefore, wireless sensor networks are 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. 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 sends the false data to the sink to cause upper-level error decision as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report wrong wildfire location information to the sink, and then expensive resources will be wasted by sending rescue workers to a non-existing or wrong wildfire location. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks.

The simultaneous flooding of false data into the sink results not only huge energy wastage in the en-route nodes but also heavy verification burdens on the sink. It could paralyze the entire network quickly. Therefore, to mitigate the energy waste, the filtering of false data should be carried out as early as possible. It is difficult to find a node once compromised while most of these filtering mechanisms use the symmetric key technique. It can be described that the compromised node abuses its keys to generate false reports and reliability of the filtering mechanisms degrade [1]

4. PROPOSED SYSTEM

In this work, the mechanism of using Bloom Filter for filtering injected false data in wireless sensor networks is proposed and it is called as bandwidth-efficient cooperative authentication (BECAN) scheme. This scheme achieves high filtering and reliability when comparing with the previously reported mechanisms. It also prevents the gangs injecting false data attack from mobile compromised sensor nodes using Ad hoc on-demand distance vector (AODV) routing protocol.

4.1 Architecture model

In this model, a typical wireless sensor network architecture is formed which consists of a sink and a large number of sensor nodes $N = \{N_0, N_1, \ldots\}$ randomly deployed at a certain interest region (CIR) is considered with the area S[1]. The sink is a data collection device which has sufficient computation and storage capabilities. The sink is responsible for initializing the sensor nodes and collecting the data.

The communication between two sensor nodes is bidirectional as their wireless transmission range (R) communicates with each other. The closer sensor node to the sink can have direct contact with sink. The farther sensor node from the transmission range of the sink has to establish the route to communicate with the sink.

4.2 En-routing

It is not possible for the attacker to generate correct MACs of other T-Nc distinct categories. The T−Nc key indices of distinct partitions and T−Nc MACs have to be forged for producing seemingly legitimate reports. To be able to detect an incorrect MAC and drop the report, the probability of a forwarding node having one of the T-Nc keys has to be computed. In this work, the Bloom filter plays a major role for computing the probability. Formation of the routing using MAC is the primary task prior to check the security of the routing. Once the security of the routing is confirmed, the forwarding of the data from node to node will take place.

4.3 EXPERIMENTS: SECURITY ANALYSIS

The main objective of this work is to effectively filtering the injected false data using BECAN authentication scheme of security analysis. The scheme of pair wise shared security for BECAN is used here. The RSA algorithm is used for generating and establishing pair wise key in this module.

4.3.1 Simulation –Based Bloom Filtering Evaluation

The bloom filtering probability is tested using simulation model as

$$FPR = \frac{\text{Number of false data filtered by en - route nodes}}{\text{Total number of false data}}$$

The results of FP_R from the simulation model are follows.

4.3.2 Simulation Settings

A Network Simulator is used to study FP_R of the BECAN scheme. In the simulations, 1,000 sensor nodes with a transmission range R are randomly deployed in a CIR of region 200 × 200 m^2 interest region. It is considered that each sensor node could be compromised with the probability ρ. The list of simulation parameters is provided in Table 1. Then, the networks are tested when the numbers of en-routing nodes in the interest areas are varied from 5 to 15 in increment of 1. For each case, 10,000 networks are randomly generated and the average of bloom filtering probabilities over all of these randomly sampled networks is reported.

Table 1. Parameter Settings

Parameter	Value
Simulation area	200m ×200m
Number of Sensor nodes	100
Transmission range R	20m,25m
Compromised Probability	2%
# Neighboring nodes k	4,6
#Routing nodes l	2,…,10
Routing Protocol	AODV
Data Rate	8.6 Mbps
Packet Size	1026 bytes
Simulation Time	100 seconds

4.3.3 Simulation Results

We have used NS-2 [16] for the simulation of the proposed scheme. Sensor network packages [17]are configured on the top of NS-2, which involves the configuration of phenomenon channel, data channel, phenomenon nodes with phenomenon routing protocol to capture real time events, phenomenon nodes pulse rate, phenomenon type, sensor nodes, non-sensor nodes, sensor agents, UDP agents, sensor applications etc. Nodes are randomly deployed into a terrain of dimension 200m X 200m. The detailed information of the simulation environment is shown in Table 1. The simulation consists of 100 sensor nodes .The routing protocol adopted in our simulation is AODV [18] (Ad hoc On demand Distance Vector). We preferred AODV as routing protocol because it does not need any central administrative system to control the routing process. Generally reactive routing protocols like AODV tend to reduce the control message overheads at the cost of increased latency in finding new routes [19]and also it reacts relatively fast to the topology changes in the network and updates only the nodes affected by these changes. It also saves storage place and energy. The destination node checks the integrity of the message m and the timestamp T. If the report is correct , the destination node forwards it to its upstream node. If the timestamp is out of date, the report (m,T,MAC) will be immediately discarded.

4.4 Sink Verification

The sink receives the report (m T MAC), checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m,T,MAC) will be immediately discarded. Otherwise, the sink looks up all private keys k_{is} of N_i,0<=i<=k , and invokes the Algorithm . If the returned value of algorithm is accepted the sink accepts the report m otherwise the sink rejects the report. The reliability of the BECAN scheme using MAC is shown in figure 2. This proposed scheme achieves 16% increase in reliability compared to previous one.

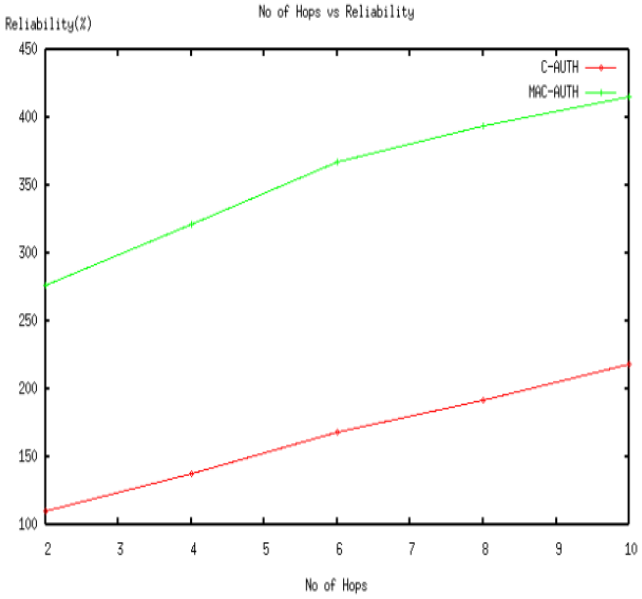

Fig 2: Reliability of the BECAN scheme

4.5 Performance Evaluation

The computational and communication overhead of the basic scheme is analyzed. Energy saving is always crucial for the lifetime of wireless sensor networks. In this module, the performance of the proposed BECAN scheme is evaluated in terms of energy efficiency. In this scheme first the security is checked, and then the throughput and delay of the packet ratio is checked. The graph analysis report is given below. The energy consumption in non interactive key pair establishment and energy consumption in transmission are evaluated. It is observed that the BECAN scheme could be applied to other fast distributed authentication scenarios. We have evaluated our proposed scheme based on Bloom filter mechanism in terms of Packet Delivery Ratio, Throughput, End to End Energy, End to

End Latency. We have found a remarkable improvement in their performances.

4.5.1 Packet Delivery Ratio

Packet Delivery Ratio (PDR) also known as the ratio of the data packets is delivered to the destinations . The PDR shows how successful a protocol performs delivering packets from source to destination. The higher value gives better results. This metric characterizes both the completeness and correctness of the routing protocol and also reliability of routing protocol by giving its effectiveness. Scenario has been set up for 100 nodes . When the simulation is started the route discovery process of AODV is done and report forwarding nodes are chosen. Now the environment is ready for the sensor nodes to sense the events and report them to their respective upstream nodes. As the simulation time progresses the malicious nodes activity ,it completely drops false injected data attack.

Hence Packet delivery ratio is analyzed in different scenarios such as in the presence of BECAN scheme without Bloom filter and in the presence of BECAN scheme with Bloom filter. It is observed to have 17 % increase in the Packet Delivery Ratio as shown in the fig. 3 after the Enroute mechanism is employed using MAC based on Bloom filter. This is why because when reports are verified by every destination node, the destination node forwards report to its upstream nodes are done , it is difficult for an attacker to forge a false injected event that has not happened. Hence through Enroute mechanism the false report is identified and thereby eliminated before they are forwarded to their destination nodes.

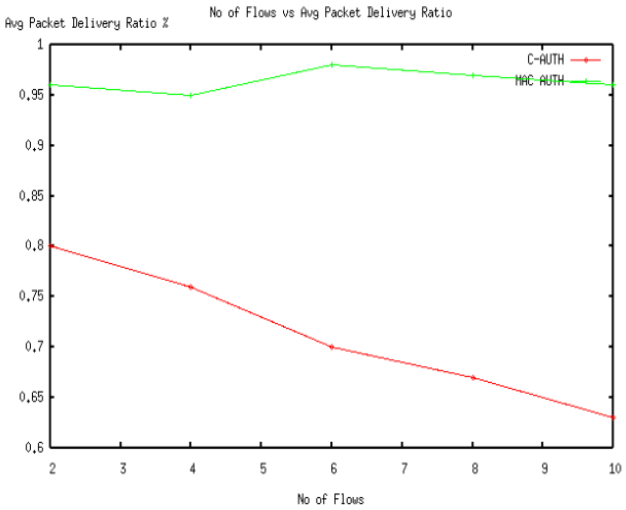

Fig 3: Performance Evaluation for Packet delivery ratio

4.5.2 Throughput

The amount of data is transferred from one place to another or processed in a specified amount of time. Throughput is defined as the average rate of successful message delivery over a communication channel or sum of the data rates that are delivered to all nodes in a network. As there is heavy packet loss with the presence of malicious activity, the throughput of the network is declined to a percentage of 40. Throughput of the network highly suffers because of False report injection attacks. False report injection attack degrades the throughput level because of the single illegitimate MAC offered to the node. There is a great vulnerability of the reports being dropped by a legitimate node. As shown in the fig. 4 Enroute Filtering mechanism achieves a throughput increase of 20% in the proposed scheme.

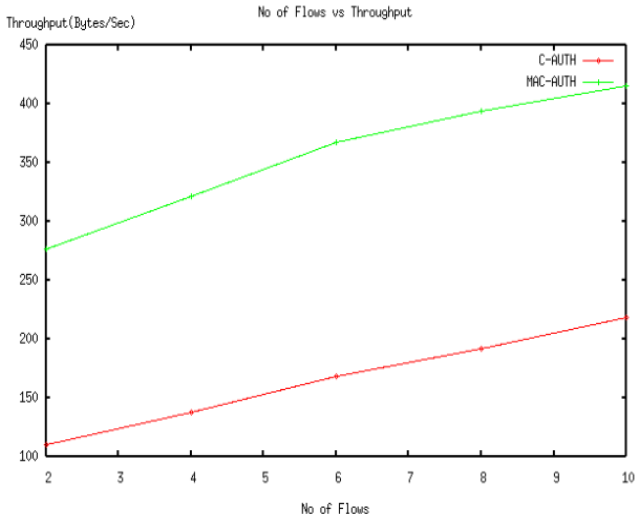

Fig 4: Performance Evaluation for Throughput

4.5.3 Average End-to-End Delay

There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times. Average end-to-end delay is an average end-to-end delay of data packets. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gives the average end-to-end delay for the received packets. This metric describes the packet delivery time, the lower the end to-end delay the better the application performance. Same scenario is maintained in which the Average End to End Delay is computed by varying the number of attackers. As shown in the fig. 6 the delay in the Enroute mechanism is found to be comparatively less than that of the normal scenario because when the destination node finds a false report in the path, it breaks the path by discarding the report. Generally reactive protocols like AODV tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. But with the proposed Enroute mechanism it is observed to have a decrease of 0.6 seconds in the reception of sensed reports to the base station.

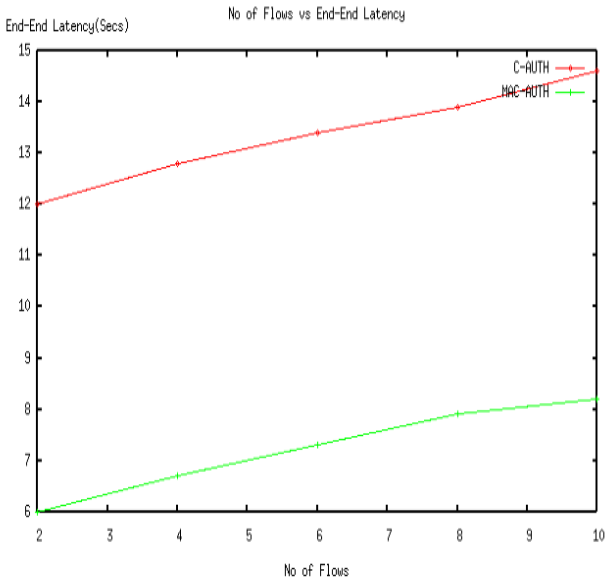

Fig 5: Performance Evaluation for End to End Latency

4.5.4 End-to-End Energy

Energy Savings. Figure 6 shows the total energy consumption for BECAN scheme using MAC. Total energy consumed for all the protocols is directly proportional to the number of transmissions, which is the sum of the number of data packets sent and the number of control packets sent per node. We propose to use a novel bandwidth-efficient cooperative authentication (BECAN) scheme that significantly reduces the energy consumption in wireless sensor networks without reducing the number of packets that meet end-to-end real-time deadlines. The proposed scheme maximizes energy savings by adaptively waiting for packets from upstream nodes to perform in-network processing without missing the real-time deadline for the data packets. We also use AODV routing protocol for nodes to adapt to network traffic to maximize energy savings in the network. Simulation results show that the proposed scheme improves the energy savings in sensor networks where events are sensed by multiple nodes and spatial or temporal correlation exists among the data packets.

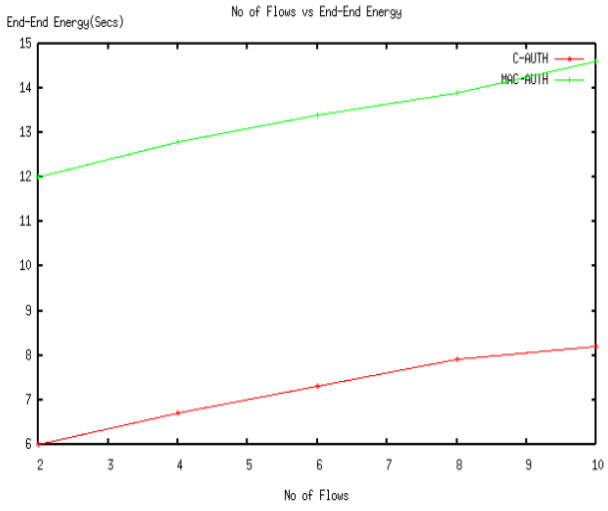

Fig 6: Performance Evaluation for End to End Energy

5. RELATED WORK

In recent years, sensor network security has been studied in number of proposals. Some of the research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have appeared in the literatures [8],[9], [10], [11], [12]. In [8], Ye et al. has proposed a statistical en-routing filtering mechanism called SEF. The SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs) and detects similar event. Each node verifies the correctness of the MACs at earliest point while the report being forwarded. Whenever the injected false data escapes from the en-routing filtering and delivered to the sink, the correctness of each MAC carried in each report is verified and rejected as false one by the sink. In SEF, each node gets a random subset of the size k keys from the global pool of size N keys to produce and verifies the MACs. SEF uses bloom filter to reduce the MAC size to save bandwidth. As estimated in the simulation, SEF can prevent the false data injection attack with 80-90 percent of probability within 10 hops. The filtering probability at each en-routing node p = k (T_Nc)/N is relatively low and SEF never considers crucial of false data filtering, the possibility of en-routing nodes' compromise.

In [9], Zhu et al. presents an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes of lower and upper association node along the path. The en-routing node forwards received report after successfully verified by its lower association node. The scheme compresses t + 1 individual MACs by XOR them to 1 in order to reduce the size of the report. The sink can detect the injected false data only after less than t nodes are compromised. In this method, security is guaranteed by the creation of associations in the association discovery phase. Zhu et al.'s scheme [7] is similar to SEF, acquired symmetric keys from a key pool and allows compromised nodes to abuse these keys to generate false report.

Yang et al. [10] proposed a Location-Based Resilient Secrecy (LBRS). This method is known as location key binding mechanism. It mitigates false data generation in wireless sensor networks and also reduces the damages due to node compromise. Ren et al. [11] proposed more efficient location-aware end-to-end data security design (LEDS) which provides end-to-end security for false data filtering. Since LEDS is a symmetric key based solution, the location-aware key management is required to achieve en-routing filtering. Zhang et al.[12] provides a location-based keys system to address this problem. This system binds individual private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms.

Chan et al.[15] proposed the use of probabilistic key sharing for establishing trust between neighboring nodes. It has similarities with SEF key assignments. Bit-compressed authentication technology based on bloom filter authentication overheads is needed to achieve en-route filtering. Similar approaches to achieve bandwidth-efficient are adopted in other works [13], [14]. Canetti et al. [13] uses one-bit authentication to achieve multicast security. The multicast approach is like BECAN scheme. In this approach, the security is based on the assumption that the source is not compromised. This scheme is not suitable for filtering false data since the scheme does not work when the source is compromised.

In this work, the proposed BECAN scheme adopts CNR based filtering mechanism together with multi reports technology. Hence it is different from above described approaches. BECAN does not require a complicated security association for non interactive key establishment [9], [11]. Also, BECAN considers the probability of some of the en-routing nodes which could be compromised. BECAN distributes the authentication of en-routing to all sensor nodes along the routing path to avoid complexity. This scheme adopts bit-compressed authentication technique to save bandwidth. The proposed technique is suitable to handle compromise and filter injected false data in wireless sensor networks.

6. CONCLUSION

In this paper, a different BECAN scheme is proposed for filtering the injected false data based on Bloom filter. This proposed approach is efficient and can be used for making theoretical analysis on relevant works. It is observed from the experiments that the BECAN scheme can achieve better en-routing filtering probability and improved reliability with multi-reports. The performance of the packet delivery ratio, end-to-end latency and throughput of the proposed system are achieved in the simulation experiments. The result shows that the proposed system impresses performance on energy consumption, security of data and also the communication cost. This BECAN can also be applied on other distributed authentication scenario since it prevents unauthorized access through injecting false data attack from mobile compromised sensor nodes through routing protocols.

7. ACKNOWLEDGMENTS

Foremost I thank Almighty Lord for success full completion of my thesis. I would like to express my sincere gratitude to my guide Dr.M.Durairaj, for his guidance. He helped me in all the time of my studies and writing of this thesis. I could not have imagined having a better advisor and mentor for my research work. Besides my guide, I would like to express my gratitude towards my coordinator Dr.E.George Dharma Prakash Raj for the continuous support of my studies and research, and for his patience, motivation, enthusiasm, and immense knowledge. Finally I thank my mother S.Mehar Nisha who always encourages for my higher studies.

8. REFERENCES

[1] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 1, January 2012.

[2] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System rchitecture Directions for Networked Sensors, SPLOS, November 2000.

[3] Nirupama Bulusu, Sanjay Jha, "Wireless Sensor Networks, A Systems Perspective",ISBN:1-58053-867-3, 2005.

[4] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

[5] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[6] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08), May 2008.

[7] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005

[8] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.

[9] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[10] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), pp. 34-45, 2005.

[11] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM '06, Apr. 2006.

[12] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 247- 260, Feb. 2006.

[13] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions," Proc. IEEE INFOCOM '99, pp. 708-716, Mar. 1999.

[14] Z. Benenson, C. Freiling, E. Hammerschmidt, S. Lucks, and L.Pimenidis, "Authenticated Query Flooding in Sensor Networks,"Security and Privacy in Dynamic Environments, Springer, pp. 38-49,July 2006.

[15] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *IEEE Symposium on Security and Privacy*,2003.

[16] "Network Simulators", [Online] Available: http://www.isi. edu/nsnam/ns/

[17] "Simulating Sensor Networks in NS-2",[Online] Available:http://nile.wpi.edu/NS/

[18] Gowrishankar, S. Subir Kumar ,Sarkar. Basavaraju, T.G. (2009),"Scenario Based Simulation Study of Ad hoc Routing Protocol's behavior in Wireless Sensor Networks", Proceedings International Conference on Future Computer and Communication, Vol.5, No.4, July 2009, pp 527- 532.

[19] Usop, N. S. M. Azizol Abdullah. Abidin, A.F.A. (2009),"Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment", International Journal of Computer Science and Network Security (IJCSNS), Vol.9 No.7, pp 261-268.