Cooperative Bit-Compressed Authentication Scheme against Compromised Node Attacks in Wireless Sensor Networks

Teenu Liza Thomas
PG Scholar, M.E.C.S
Hindusthan College of Engineering and Technology Tamilnadu, India

P. Vijayalakshmi
Associate Professor, ECE
Hindusthan College of Engineering and Technology Tamilnadu, India.

ABSTRACT
Sensor nodes deployed at hostile environments suffer compromise node attacks, in which an adversary injects counterfeit data into the sink causing error detection at upper level and energy wastage in en-route sensor nodes. A novel authentication scheme known as, Cooperative Bit-Compressed Authentication (CBA) is based on random graph characteristic of sensor node deployment and a cooperative bit-compressed authentication scenario with probability of neighboring nodes providing the necessary condition for CBA authentication. In this safest en-route is found out using client puzzle. Early detection and filtering of injected false data with CBA technique greatly saves energy adding a minor extra overhead at the en-route sensor nodes. The accompanied authentication information is bandwidth-efficient. Filtering of false data reduces the burden of the sink and in addition only very small fraction of injected bogus data needs to be checked by the sink. The high filtering probability, high reliability, throughput and energy saving of the CBA scheme is demonstrated in simulation results.

General Terms
Cooperative Bit-Compressed Authentication(CBA)

Keywords
Wireless sensor networks, cooperative bit-compressed authentication, false data injection, en-route filtering.

1. INTRODUCTION
Wireless Sensor Networks deploy large number of sensor nodes and sink. Sensor nodes sense environment changes and report to other nodes over a transmission range within the network architecture. During initialisation and deployment large number of sensor nodes are randomly deployed at a certain interest region (CIR) within an area. Sink is a powerful and trustable data collection node, which has high computation and storage capabilities and is responsible for initialising sensor nodes and collecting sensed data. Sensor nodes which are stationary in location have non-zero identifier. Communication is bi-directional within their wireless transmission range (R). Sensor nodes can communicate with each other within R. Sensor node close to sink, directly contact the sink and which is far away from the sink within the transmission range resort to other nodes to establish route and communicate with sink. During non-transmission periods after deployment the sensor nodes uses routing protocol like AODV to find out the shortest path sink and this can accelerate the reporting.

1. Compromised Node Attacks
Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks—for example, falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. Addressing the problem of sensor node compromise requires technological solutions. For example, cheap tamper- resistant hardware could make it challenging to reprogram captured sensor nodes. However, making nodes robust to tampering is not economically viable. We must therefore assume that an attacker can compromise a subset of the sensor nodes. Hence, at the software level, sensor networks need new capabilities to ensure secure operation even in the presence of a small number of malicious network nodes. Node-to-node authentication is one basic building block for enabling network nodes to prove their identity to each other. Node revocation can then exclude malicious nodes. Achieving these goals on resource limited hardware will require lightweight security protocols. Further, all communications and data-processing protocols used in sensor networks must be made resilient—that is, able to function at high effectiveness even with a small number of malicious nodes. For example, routing protocols must be resilient against compromised nodes that behave maliciously.

2. DESIGN GOAL
The design goal is to develop a cooperative bit-compressed authentication scheme against compromised node attacks in a secure and energy efficient manner. The two objectives achieved are

1. Energy Saving by Early Detection of Injected False Data.
The authentication task in CBA scheme has the capability of early detection of false data. This can greatly reduce the energy consumption at the en-route nodes. If the entire authentication task is fulfilled by the sink, this greatly increases the burden of the sink and can bottleneck the sink. The authentication by en-route sensor node helps in early detection of injected false data and thus can save energy adding a minor overhead at the en-route sensor node.

2. Achieving Bit-Compressed Authentication.
A Message Authentication Code (MAC) is produced so as to authenticate the transmitted data through the en-route nodes. MAC is one bit, thus making bit-compressed authentication possible.

3. METHODOLOGY

The framework for the proposed scheme for CBA authentication is shown in Figure 1.

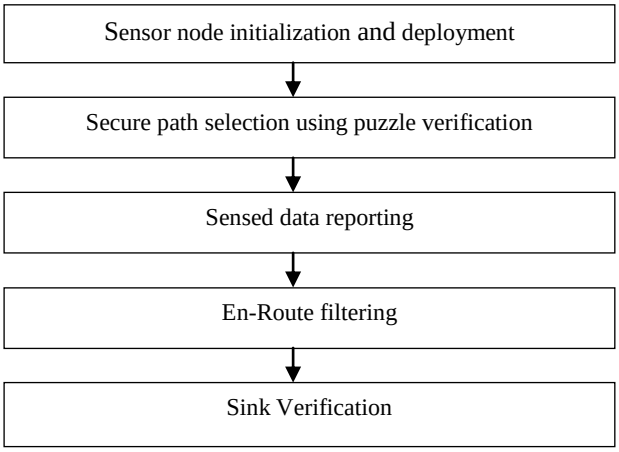

Fig 1: Steps in CBA authentication

Sensor nodes are initialized and deployed. Followed by the detection of shortest and safest path using puzzle verification, then using proposed authentication scheme sensed data is authenticated and verified which is discussed in the following section and finally the performance is analysed.

4. PROPOSED AUTHENTICATION SCHEME

A Cooperative Bit-Compressed Authentication (CBA) scheme for filtering injected false data in Wireless Sensor Networks (WSN) has been proposed. The two main phases are:

A. Safe path selection.
B. Authentication and verification of sensed data.

4.1 Sensor node initialization and deployment.

All sensor node are uniformly and randomly deployed at CIR. When the sensor nodes are not involved in reporting task, they cooperatively establish shortest path, by AODV routing protocol. This can accelerate reporting of sensed data.

STEP1 : Choose the number of sensor nodes.

STEP2 : Store the location of each sensor node.
STEP3 : Preload each sensor node with public key.

STEP4 : Choose the shortest path using AODV routing protocol.

4.2 Secure path selection using puzzle verification.

For safe data transmission the transmission path should be adversary free i.e., there should be secure path. All the sensor node in the shortest path should be able to solve the cryptographic puzzle[8] given to them using the key given to them during initialization phase inorder to be recognized as a secure node in the shortest path selected. Puzzles are accompanied by certain time outs during which the specific node should be able to solve the puzzle.

STEP1 : Distribution of cryptographic puzzle to the sensor nodes in the shortest path between the source and destination selected during initialization.

STEP2 : Solve the puzzle within the specific time interval.

4.3 Sensed data reporting.

The report *R* generated by sensor node by sensing of any parameters are send to the sink via, established shortest and safest path selected.

STEP1 : Source node attains time stamp T, chooses *m* neighboring nodes and send the report *R* to the sink via routing nodes.

STEP2 : Each en-route sensor node on receiving *R* generate *mac*.

STEP3 :*mac* generated by en-route neighboring nodes generate row authentication vector.

$$Row_i = (mac_{i1}, mac_{i2}, mac_{i3} \ldots\ldots mac_{il}, mac_{is}) \quad (1)$$

STEP4 : All the row vectors $(Row_0, Row_1 \ldots\ldots Row_k)$ are aggregated
to form the MAC authentication information.

$$MAC = \begin{pmatrix} Row_0 \\ Row_1 \\ \vdots \\ Row_k \end{pmatrix} = \begin{pmatrix} mac_{01} & \cdots & mac_{0s} \\ \vdots & \ddots & \vdots \\ mac_{k1} & \cdots & mac_{ks} \end{pmatrix} \quad (2)$$

4.4 En-Route filtering.

Each en-route sensor node checks the integrity of the report, *R* and the time stamp T. If T is outdated, the report is discarded otherwise cooperative neighbor based *mac* verification is done.

STEP1 : Checks the timestamp T.

STEP2 : Each en-route sensor node uses noninteractive keypair establishment to compute shared keys with each sensor node.

STEP3 : If *R* is cooperatively authenticated by k neighbor nodes the report is MAC verified.

4.5 Sink verification.

Sink on receiving the report checks the integrity of *R* and timestamp T. If T is outdated *R* is rejected otherwise *R* undergoes sink verification.

STEP1 : Checks the timestamp T.

STEP2 : Sink looks up all private keys $k_{is.}$

5. SECURITY ANALYSIS

Since the position of the sensor node is stored during the initialization phase the adversary cannot launch compromise node attack, where a group of nodes are controlled and moved by the adversary. The position information also greatly reduces reaffiliations per unit time. The report embedded with timestamp T resist replay attack. The energy consumption also reduces with short route paths, this implies scalability of CBA scheme

6. RESULTS AND DISCUSSION

A CBA scheme for filtering injected false data and preventing compromise node attacks had been analyzed. By theoretical analysis and simulation evaluation, the CBA scheme has been demonstrated to achieve not only high en-routing filtering probability but also high scalability.

Table 1. Parameter setting

Parameter	Value
Simulation area	1200 × 1200
Number of sensor nodes	100
Transmission range	15m, 20m
Neighboring nodes	4,6
Routing nodes	5,…..,15

6.1 False Negative Rate (FNR).

$$FNR = \frac{\text{Number of true data that cannot reach the sink}}{\text{Total number of true data}}$$

If FNR is small, the CBA scheme demonstrated has high reliability.

6.2 En-Route Filtering Probability (FPR).

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

The en-routing filtering probability FPR in terms of different number of en-routing nodes. As the number of routing nodes increases, FPR increases.

6.3 Reaffiliations per unit time.

Reaffiliations per unit time implies the redundancy of transmitted data.

6.4 Throughput.

$$\text{Throughput} = \frac{\text{Number of packet received}}{\text{Time}}$$

CBA scheme demonstrates to have high throughput.

6.5 Energy consumption.

The majority of injected false data can be filtered by CBA scheme within short number of hops during transmission. Thus, CBA can greatly save the energy of sensor nodes along the routing path.

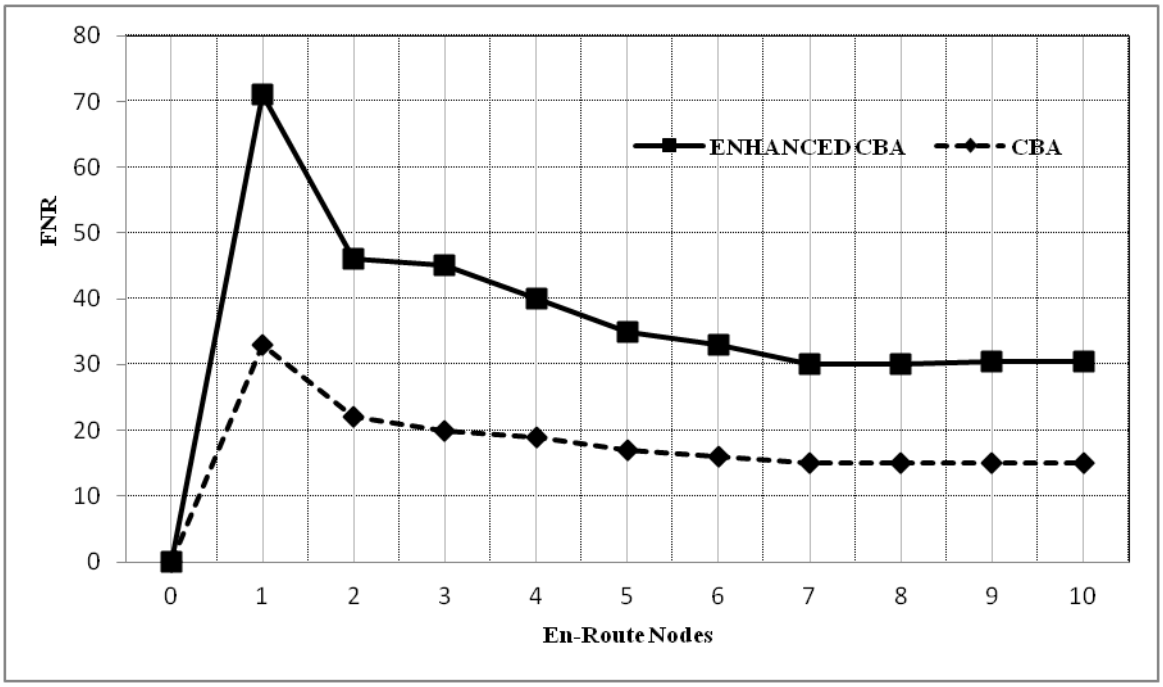

Fig 2: False Negative Rate (FNR)

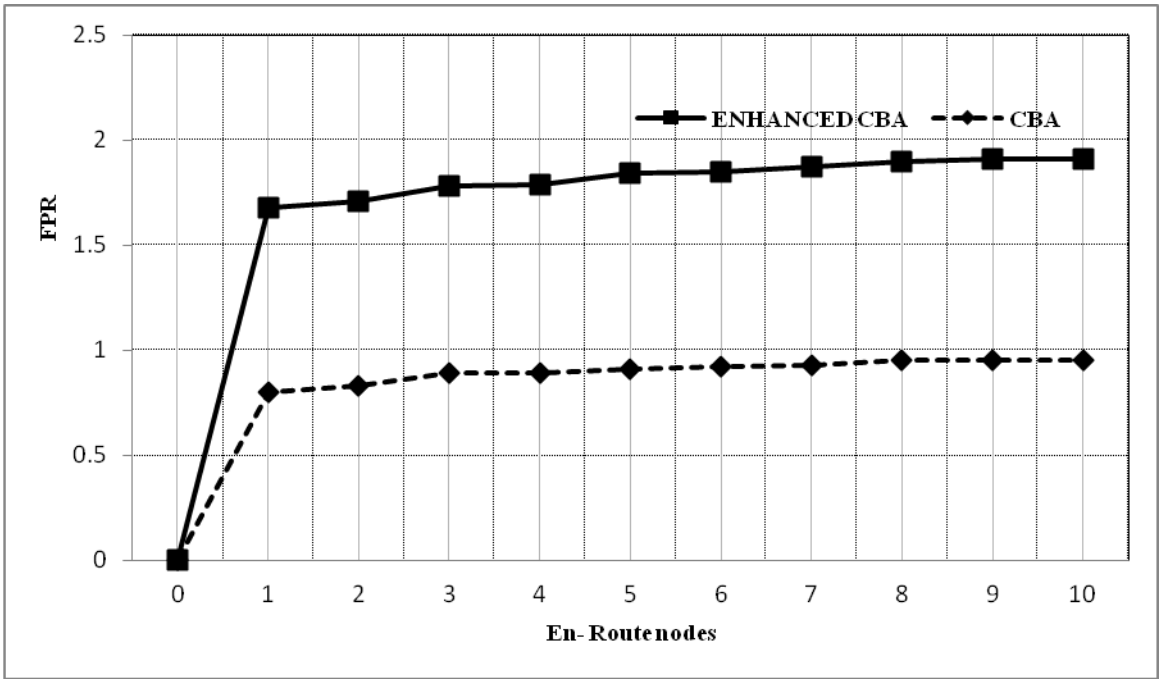

Fig 3: FPR versus different number of routing nodes *l*

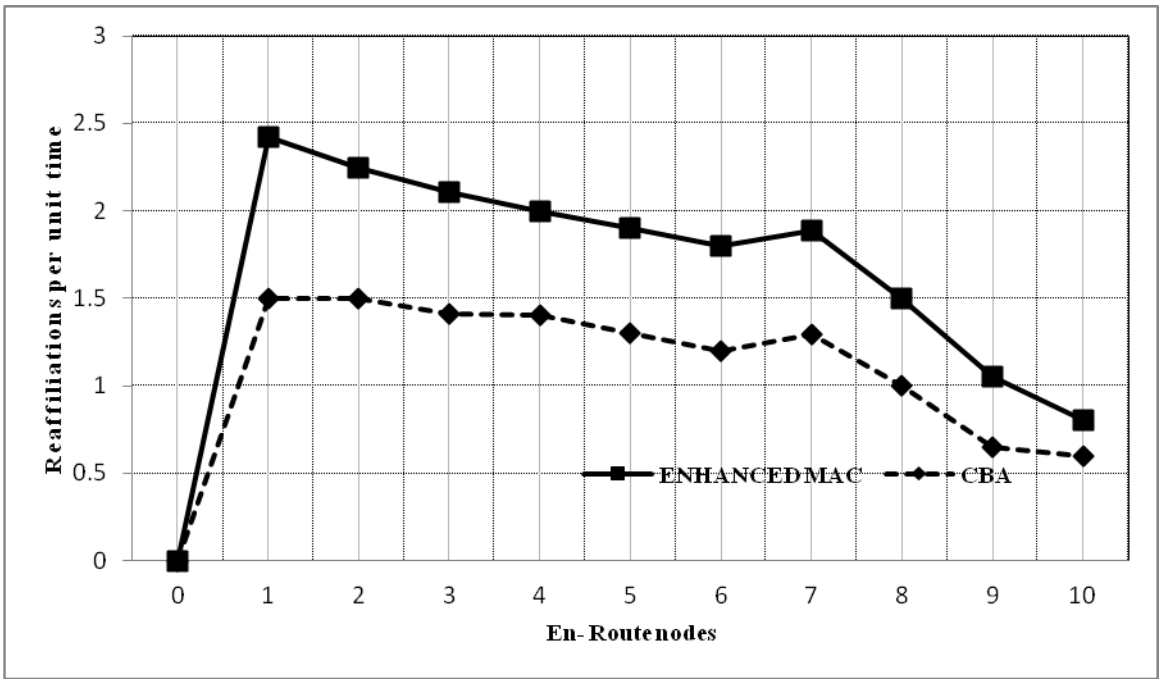

Fig 4: Reaffiliations per unit time verses en-route nodes

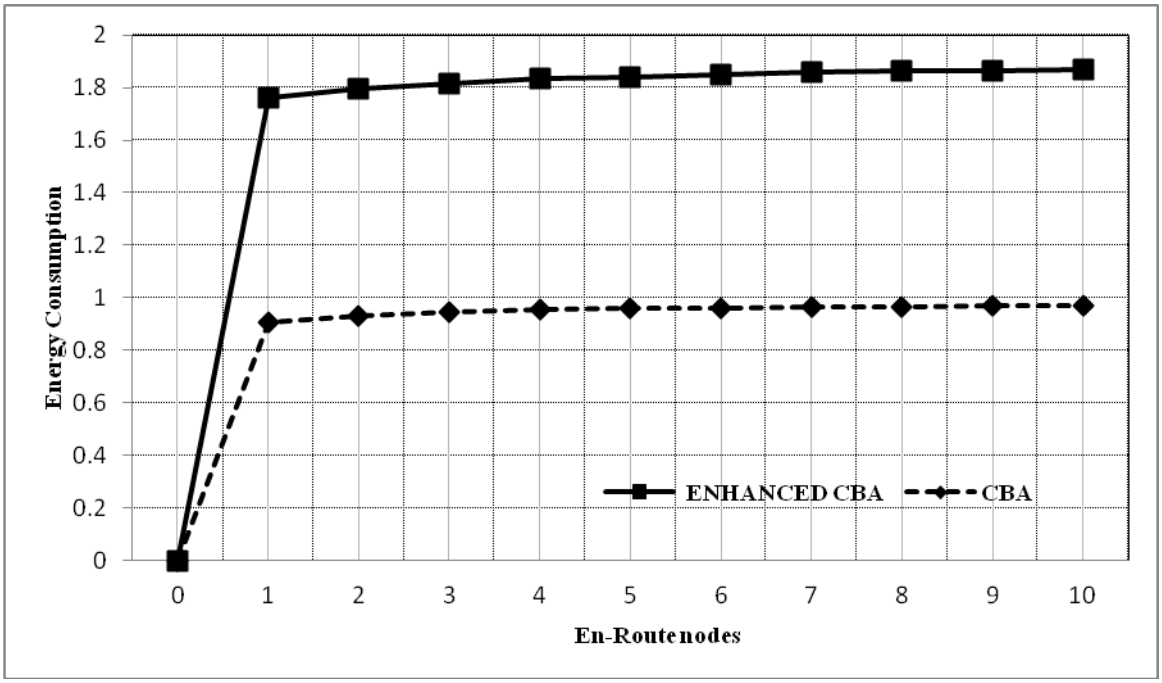

Fig 5: Energy consumed at en-route nodes

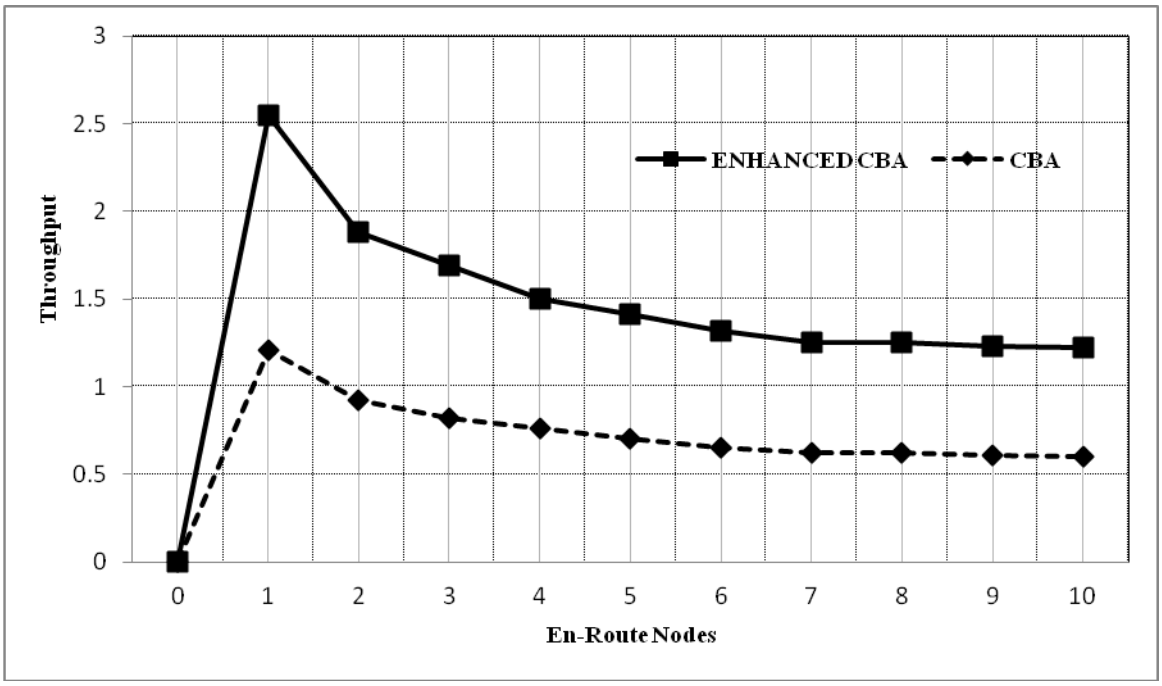

Fig 6: Throughput of CBA scheme

7. RELATED WORK

Recently, some research work on bandwidth efficient authentication have been appeared in literature BECAN [1]. Here compromise probability of sensor node is taken into consideration. Much of the attention is paid to make the scheme bandwidth efficient. A statistical en-route filtering mechanism known as SEF was proposed in [5]. In SEF the report is validated by multiple keyed MAC. In [10] an IHA scheme is proposed in which each node is associated with two other nodes in the routing path and in which the report is forwarded if it is verified by the lower associated node.

8. CONCLUSION

The proposed CBA scheme is a novel scheme for filtering the injected false data and to prevent compromise node attacks. This scheme is demonstrated to have high en-route filtering probability. CBA scheme saves energy by early detection of injected false data at the en-route sensor node and also provide

authentication to legitimate sensed data. Shortest and safe path selection also help to fast reporting of sensed data and energy saving. CBA scheme can be applied to applications, where security of data is of high concern.

9. ACKNOWLEDGMENTS

Authors would like to thank all the researchers who have contributed in this field of research. The comments of anonymous reviewers to improve the quality of this paper are also acknowledged.

10. REFERENCES

[1] Rongxing Lu. and Xiaodong Lin., "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, Jan. 2012.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[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] Daojing He and Sammy Chan, "DiCode: DoS Resistant and Distributed Code Dissemination in Wireless Sensor Networks," IEEE transaction on wireless communication, vol. 11, No. 5, May 2012.

[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] C. Boyd, W. Mao, and K.G. Paterson, "Key Agreement Using Statically Keyed Authenticators," Proc. Second Int'l Conf. Applied Cryptography and Network Security C (ACNS '04), pp. 248-262, 2004.

[11] J. Black and P. Rogaway, "Cbc Macs for Arbitrary-Length Messages: the Three-Key Constructions," J. Cryptology, vol. 18, no. 2, pp. 111-131, 2005.

[12] W. Mao, Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003.