Draining injected invalid data for efficient bandwidth consumption using authentication scheme in WSN

Mukul Pratap Singh*, Kunal Gupta**

*Amity School of Engineering & Technology, Noida UP
**Amity School of Engineering & Technology, Noida UP

Abstract: Wireless sensor is the biggest researching area. Now days most of the applications are working on wireless medium. In wireless sensor network Injecting invalid data attack is very serious threat. If invalid data is stored in sink than due to error decision waste of energy and bandwidth will take place. In this paper presenting a new scheme for wireless sensor network which is help in power optimization and efficient bandwidth consumption base on message authentication code (MAC). This Scheme theoretical and results are helping in the WSN application areas and improves the performance and accuracy through draining the injected invalid data.

***Index Terms*:** Power optimization, efficient bandwidth consumption, MAC, Invalid data, Private Key, WSN

I. INTRODUCTION

In recent years Wireless sensor networks are immensely used in high level and very sensitive application areas such as environmental, surveillance, habitat monitoring and tracking for military. Now we are interact various new applications at the unprecedented level from the help of Wireless sensor networks. Because these are very sensitive areas so we should make sure these networks are highly secured from invalid data attack, security attack and Sybil attacks and detection of these invalid data is very big research challenge. Interconnect large number of sensors node composed a Wireless sensor network through wireless links. If changes in temperature or light occur a sensor node is triggered and create a report which is send to data collection unit through a path, this data collection unit is called SINK.

From Injecting invalid data attack, WSNs may also suffer. If wrong data is stored in the sink than many errors can take place at higher level due to these error decisions as well as a lot of energy will be lost. For example if In weather forecasting temperature sensors or pressure sensor send the invalid information report to the sink then costly resources and precious time will be wasted in the process of forecasting. Thus it is very important to drain the invalid data as precisely as possible in WSNs. If the sink is flooded with all invalid data then as a result of it, immense load will be increased on the sink and vast energy will also be wasted. Due to which the network can be paralyzed very soon. Hence in order to save the energy and bandwidth from being wasted invalid data draining should be performing at very early stage.

To handle this challenge in this paper, we propose a new scheme for draining the invalid data in WSN. High draining probability as well as high reliability provide by this new scheme. Propose a new scheme to draining the injected invalid data with message authentication technique using private key. This proposed mechanism we can discover the invalid data sooner and drained this invalid data. And results show the effectiveness of the proposed scheme.

The paper is organized as follows, Section I: introduce the injected invalid data problem in wireless sensor networks, Section II: network model of wireless sensors. Section III: Shows which functions are achieved by the proposed scheme. Section IV: describe the proposed message authentication scheme for draining the injected invalid data for wireless sensor networks. Section V describes the data flow diagram and algorithm used in this authentication scheme. Section VI is shows the result and performance of this authentication scheme for power saving in wireless sensor networks.

II. NETWORK MODEL

A huge number of sensor nodes and a sink (Sink is an effective data accumulation unit and storage capacity, which is responsible for initializing the sensor nodes and accumulation the data) makes a distinctive wireless sensor network.

Every sensor node has a stationary position. By connecting the sensors we are making the network which leads to the Sink and send the information of triggered event through the sensor nodes. The neighbour node of sink will send the report directly and non-neighbour node will connect via other sensor node to the sink.

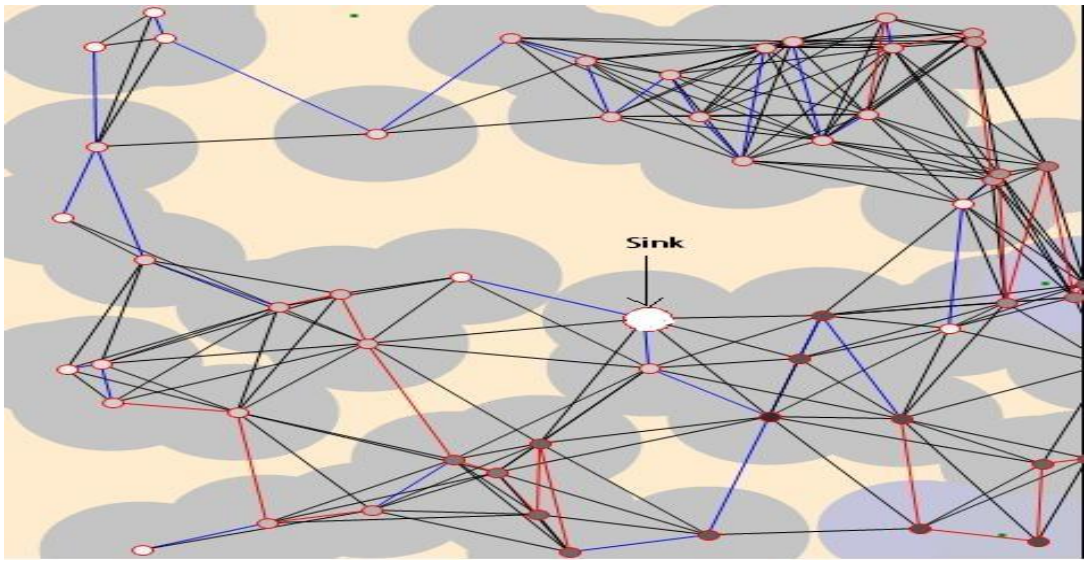


Figure 1: Network model

III. DESIGN GOAL

By develop a new authentication scheme for draining the injected invalid data following desirable objectives will be achieved.

Quickly detecting the injected invalid data
A powerful data storage device is called SINK. A sink is a bottleneck as all authentication tasks are fulfilled at the sink, we detect the invalid data before it reached to the sink because if invalid data reached to the sink then it will occur problems in the high level applications. In this paper we are detecting the invalid data at the source node. To save more energy and bandwidth of entire network, invalid data detected at initial stage.

Accomplish the Draining the Invalid data process.
After the quickly detecting the injected invalid data process we can accomplish the task of draining invalid data.

Accomplish a scheme to save from Gang Injecting Invalid Data Attack
If too many invalid data reached the sink than sink will affected from DoS (Denial of Service) attack. While more than one invalid data or a gang of invalid data aggregate at the source node and attack to the sink than it will be called gang injecting invalid data attack. Due to mobilization the gang injecting invalid data attack is hard to resist and more challenging. And by this authentication scheme we obtain the goal of protecting from gang injecting invalid data attack.

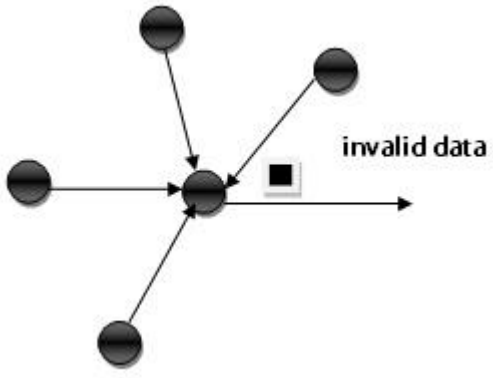


Figure 2: Gang Injecting Invalid Data Attack

IV. PROPOSED AUTHENTICATION SCHEME BASED POWER OPTIMIZATION TECHNIQUE

This technique is use for draining the injected invalid data from wireless sensor network and save the power in WSN. In this technique Message Authentication code is used. Message authentication code (MAC) provides knowledge to the recipient of the message which came from the expected sender and has not been altered in transit.

Let h (.) be a secure cryptographic hash function. A MAC in Z2^n can be considered as a keyed hash [13], and defined as

$$MAC(m, k, n) = h(m||k) \bmod 2^n$$

Where m, k, n are a message, a key, and an adjustable parameter, respectively. When n = 1, MAC (m, k, 1) provides one-bit authentication, which can filter a false message with the probability 1/2; while n = α, MAC (m, k, α) can filter an invalid message with a higher probability 1− ½^α .
To draining the invalid data injected by settled sensor nodes, this authentication scheme adopts neighbour router based draining mechanism. As shown in fig,

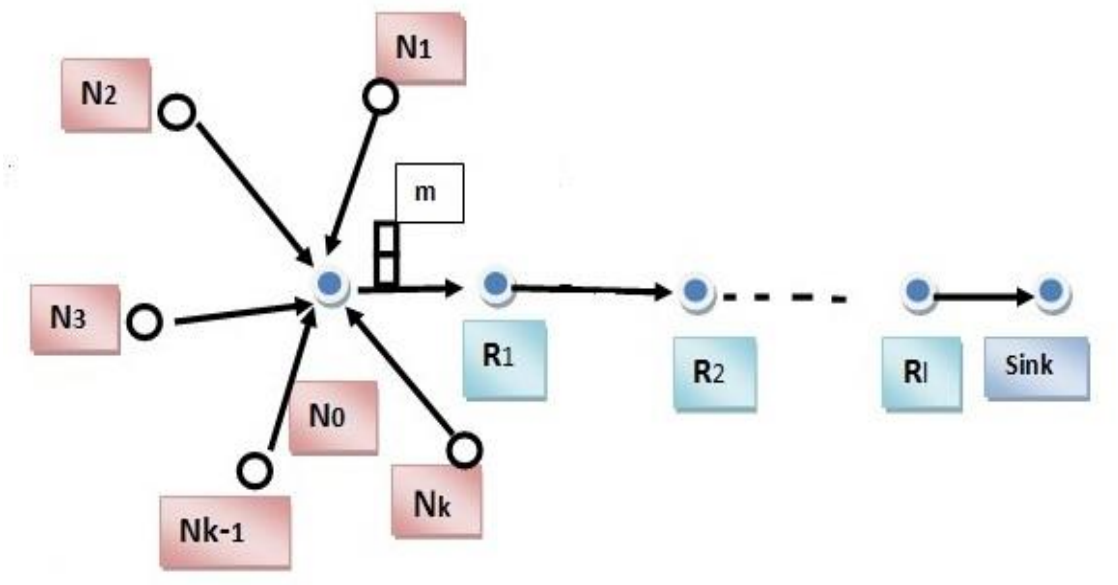
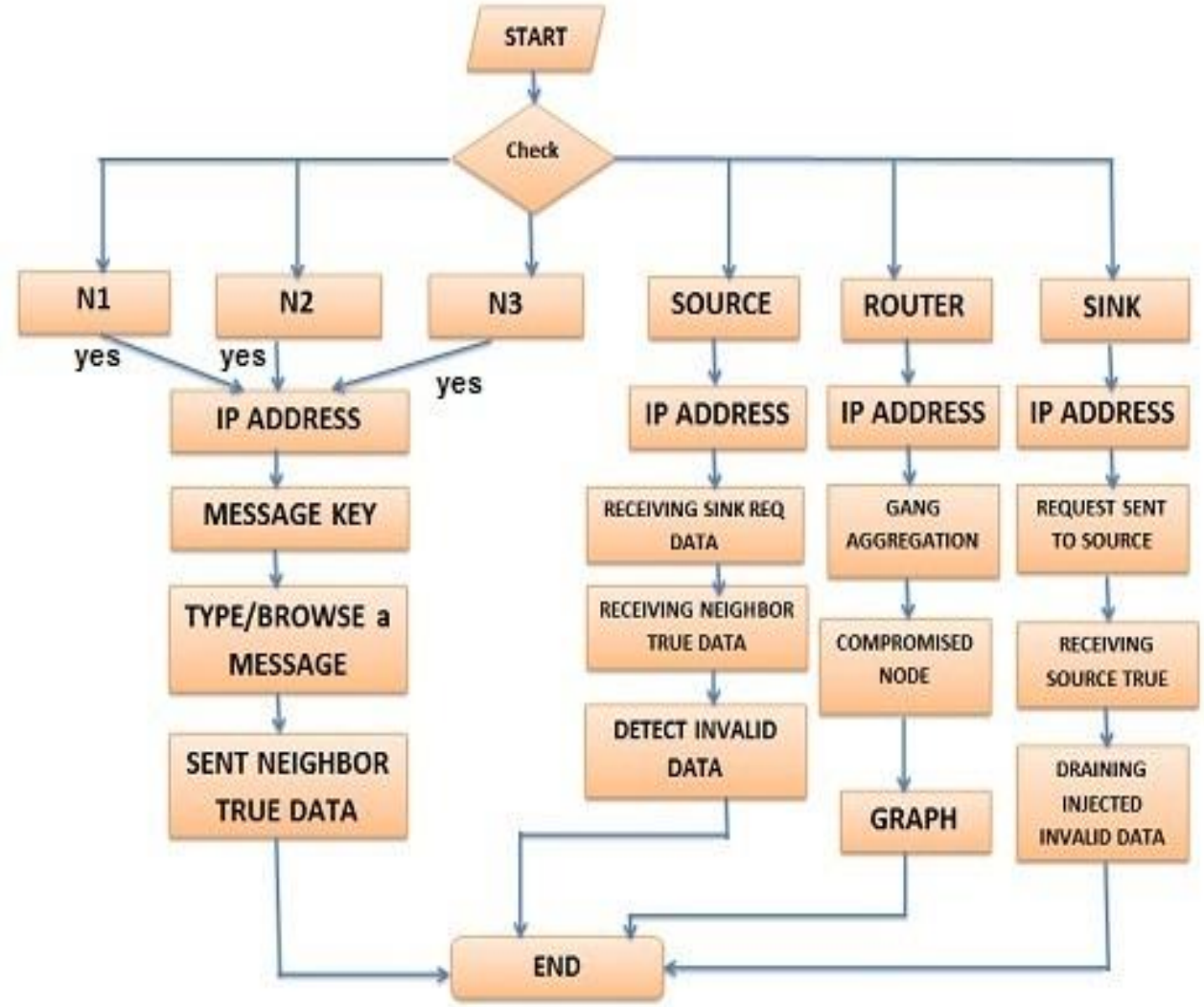


Figure 3: Neighbour router based authentication mechanism

In this mechanism, firstly set up a routing path between source node N0 and sink through $R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_1 \rightarrow$ Sink. Each sensor (N_1, N_2, N_3, N_4,..N_k) send own report m (if any change of sensor event such as temp change, pressure change, etc., this information is called report.) to source node N_0 and this report m and authentication information Message authentication code send to the sink via routing path. Every sensor node has own private key and this key also shared with the sink. From the relationship between neighbour & source node, Consorting to the Elliptic Curve Cryptography based key pair establishment, established a relationship between sink & source, source & neighbours and sink & routers. When a sensor node send an invalid reports to the source node, it will be detected at source node and drained before it reaches the sink.

I. BLOCK DIAGRAM & ALGORITHMS



Block Diagram

Procedure of the message authentication scheme

1. Start process.
2. Create six nodes Neighbor1 (N_1), Neighbor2 (N_2), Neighbor3 (N_3), Source node, Router node, Sink node.
3. Assign the IP address to every node.
4. Assign a message subject (Message key) to every neighbor node individually, and the sink has all the keys.
5. Browse the massage to N_1, N_2, N_3 and transform to the source node.
6. Source node receives all the messages from N_1, N_2, N_3 nodes.
7. Sink node request to source node for true data.
8. On the source node we detect the invalid data and send to the sink node.
9. Receiving the true data from Source node through router.
10. On sink node we obtain drained injected invalid data.
11. End Process

Used Algorithm

Algorithm 1 : With (m, T,RN_0) as input, each sensor node Ni ∈ (NN_0 ∪ {N_0}) invokes the Algorithm 1 to generate a row authentication vector) and reports Row_i to the source node N_0.

MAC Generation
1: **procedure** MACGENERATION
Input: Ni ∈ (NN_0 ∪ N_0), m, k_i,R_{N0}
Output: Key
2: Every neighbour node (N1,N2, N3,….Nk)is connected with the sink node (S) through Route(R1,R2, R3….RL) and Private key of every neighbour node(ki1,ki2,ki3…kis) shared with the SINK node.
3. **if** neighbour sends the event triggered report m to the source node
then source node detects correct report m.

Algorithm 2 : If the returned value of Algorithm 2 is "accept", the sink accepts the report m; otherwise, the sink rejects the report.

Sink Verification

1. **procedure** SINKVERIFACTION
   Input: N_k, S_k, m
   Output: accept or reject
2. if(Neighbour node key N_k = SINK node key S_k)
3. return value = "report m accept "
4. else
5. return value = "report m reject"
6. **end if**
7. **end else**
8. **return** return value
9. **end procedure**

V. RESULTS

Following figure shows the route which is complete path from source to sink node with true data and it removes the gang injecting invalid data attack. Green nodes are selected for the establishing the complete path with the sink. Red nodes are showing detected invalid data and the purple node not selected in the further event and drained the invalid data before it received by the sink. By draining the invalid data we saved more energy and bandwidth of network, which was going in vain.

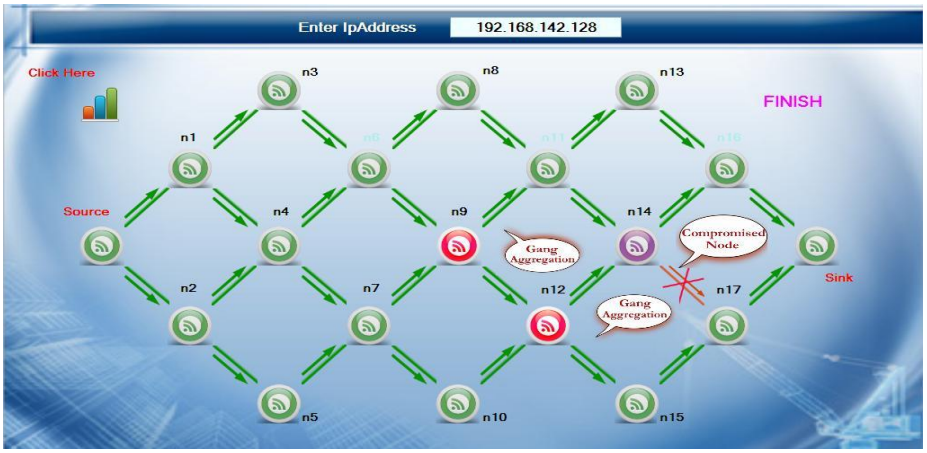


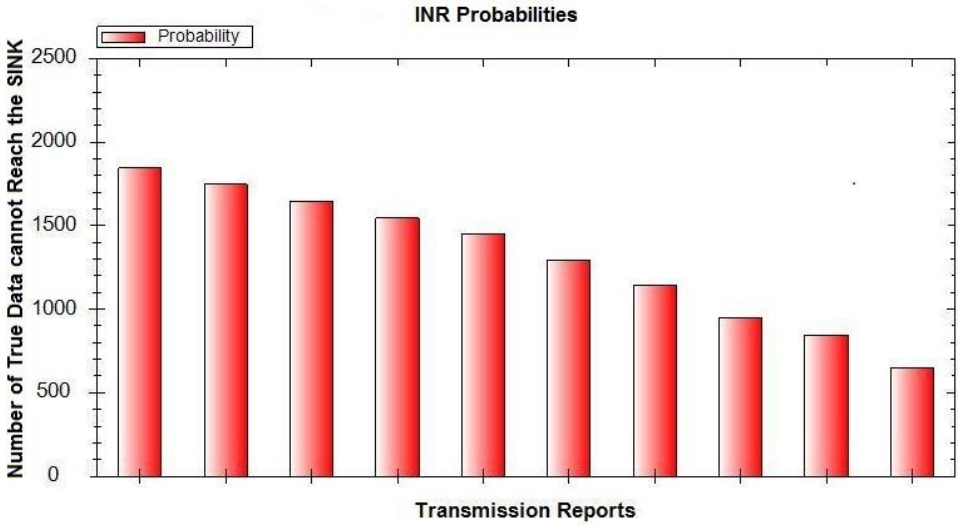
Figure 4: Complete path from source to sink node with true data

Invalid Negative Rate (INR) shows the high reliability of true data received by the sink. This Authentication scheme provides high draining probability with the high reliability.
For the testing of reliability of this scheme we use following

INR =N_t/T

N_t =Number of true data that cannot reach the *sink*
T= Total number of true data

If N_t is small than INR will decrease and small INR shows higher reliability**.** This figure shows the INR probabilities between Number of true data that cannot reach the sink and transmission Report. That figure shows that if Number of true data that cannot reach the sink is decrease than INR ratio is decrease**.**



Graph: INR probabilities

VI. CONCLUSION & FUTURE WORK

In this paper, proposed an authentication scheme for draining the injected invalid data. . The power and communication of data are the main problems of a wireless sensor network. With its limitations, it is important to design a network that uses optimal energy resources while transferring reliable data and bandwidth will be saved. By results this scheme has been achieve high reliability and high en-routing filtering probability with multi report.

This scheme is simple and effective, that it could be used in mobile sensor node authentication scenarios. In future work, we will apply this scheme while gang injecting invalid data attack on mobile sensor networks.

ACKNOWLEDGEMENT

I am very thankful to my guide Mr. Kunal Gupta, who helped me to prepare this paper. I also express my gratitude to all my friends. I never forget those who gave me the idea to prepare and submit this research paper in IJSRP prestigious journal.

REFERENCES

[1] Mukul Pratap Singh , Kunal Gupta "Techniques of Power Optimization for Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887) Volume 66– No.3,pp. 13-17 March 2013.

[2] D.Culler, D.Estrin and M.Srivastava, "Overview of Sensor Networks", IEEE Computer Society, August 2004.

[3] Fengchao Chen," Single sink node placement strategy in wireless sensor networks" Electric Information and Control Engineering (ICEICE), 2011 International Conference on,15-17 April 2011

[4] Zheng Wang, Xiaodong Lee, Xinchang Zhang and Baoping Yan," In-Field Attack Proof of Injected False Data in Sensor Networks" Journal of communications, vol. 3, no. 6, november 2008.

[5] Priyanka S. Fulare, Nikita Chavhan "False Data Detection in Wireless Sensor Network with Secure communication" International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1, Issue-1, 2011.

[6] Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. SenSys, 2003, pp. 255–265.

[7]] Eltoweissy M, Moharrum M, and Mukkamala R, "Dynamic key management in sensor networks", IEEE Communications Magazine, 2006, 44(4): pp.122-130.

[8] Younis M, Ghumman K, and Eltoweissy M, "Location- Aware combinatorial key management scheme for clustered sensor networks", IEEE Trans. on Parallel and Distribution System, 2006, 17(8): pp.865-882.

[9] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks," Proc. of the IEEE SSP 2004.

IEEE Computer Society Press, 2004: pp.259-271.

[10] D. Seetharam and S. Rhee, "An efficient pseudo random number generator for low power sensor networks," in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004,

pp. 560–562.

First Author-Mukul Pratap Singh (M.Tech-CSE) Amity School of Engineering & Technology, Amity University, Noida(UP),singh.mukulpratap@gmail.com .

Second Author- Mr. Kunal Gupta (Assistant Professor) Amity School of Engineering & Technology, Amity University, Noida(UP) kunal2151@gmail.com