International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

PRESERVATION OF SINK-NODE LOCATION IN WSN FOR SDN PARADIGM

Shreenidhi S Hegde[1],Sridhar H A[2], Shashank D[3]

[1]BE, VIII Sem, Dept. of ISE,The National Institute of Engineering, Mysuru
[2]BE, VIII Sem, Dept. of ISE,The National Institute of Engineering, Mysuru
[3]Asst. professor, Dept. of ISE,The National Institute of Engineering, Mysuru

---

Abstract—***A Wireless Sensor Network (WSN) is a network which contains autonomous devices which are distributed spatially over an area. The sensor nodes in it will be having the potential to sense the environmental conditions and monitor them like Environmental monitoring of air, water, soil , structural monitoring of buildings and bridges, industrial machine monitoring , process monitoring , asset tracking etc. A WSN node contains many components like radio, battery, microcontroller, analog circuit, and sensor interface. It is difficult to adequately address source-location privacy (SLP) in WSN. SLP service is further complicated by the nature that the sensor nodes generally consist of low-cost and low-power radio devices. This paper explains the implementation of AODV protocol we are proposing.***

I. INTRODUCTION:

Wireless sensor network (WSN) is a system of network spatially distributed devices using wireless sensor nodes to sense environmental or physical conditions. The Individual nodes are competent of sensing their environments and sending data to one or more compilation Points in a WSN. One of the most significant issues for WSNs is efficient data transmission

A. Sinkhole attack

an intruder compromises a node or introduces a new node inside the network and uses it for sinkhole attack. The compromised node tries to attract all the traffic from neighbor nodes based on the routing metric used in the routing protocol. When the compromised node manages to achieve that, it will launch an attack. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Many nodes send data to a single station in the ad hoc network and many to one pattern of wireless sensor networks communication where WSNs are particularly vulnerable to sinkhole attacks. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only those close to the base station. We consider two scenarios of sinkhole attacks. Initially intruder has more power than remaining nodes. In the second the intruder and other nodes have the same power. In all the above mentioned cases the intruder claims to have the shortest path to base station,hence it can attract network traffic. In a wireless sensor network the best path to the base station is the basic metric for routing data

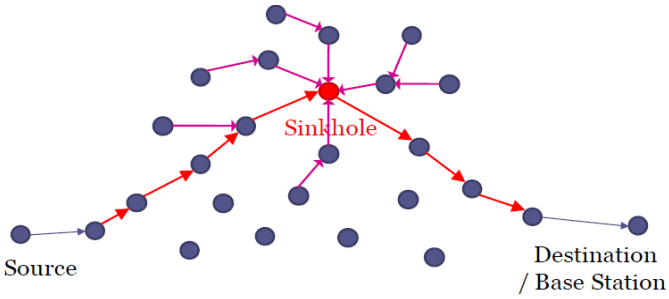


Fig1. Scenario of sinkhole attack in WSN

B. Clustering technology

Clustering divides nodes into groups which are called clusters. Each cluster is managed by a cluster head and all members are Co-ordinated with the cluster head. communication between the members and cluster heads are the responsibilities of the cluster head. There are diverse methods for selecting cluster head. In some methods cluster head is selected by cluster members; while, in other methods cluster head is selected by network designer. Cluster head can be same or change based on the algorithm. The same is true for members of clusters. In clustering methods each sensor is either a cluster head which introduces itself in a specific region or is a member which must introduce itself to cluster head and become its member. The members are

allowed to communicate with their own cluster head and transmit

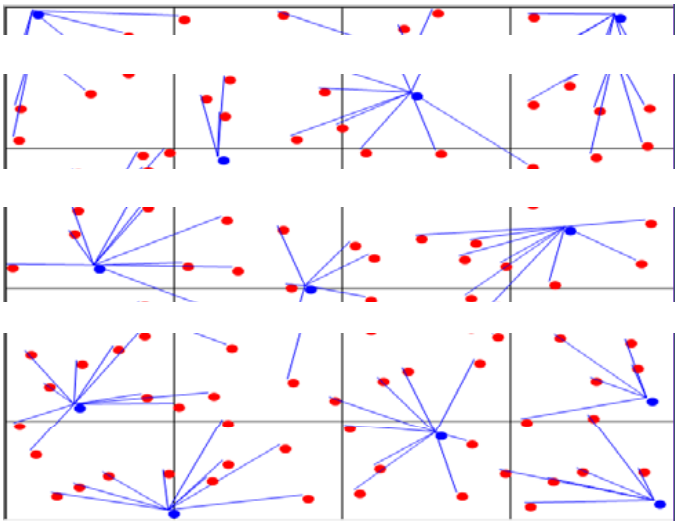


Fig 2. Clustered wireless network.

II. EXISTING SYSTEM

In existing system the mobile agent technology based security solution against sinkhole attack for wireless sensor networks(WSNs). WSN has a dynamic topology, intermittent connectivity, and resource constrained device nodes. Mobile agent is self-controlling programming agent. They traverse from node to node while transmitting data and doing computation. They are many methods for distributed applications, and especially for a dynamic network environment. This mechanism does not require more energy .Sinkhole attacks are work by making a compromised node look especially attracts network traffic by advertising fake routing updates. This fake updates are creates opportunities for attackers. So we want to detect and avoid sinkhole attack, many different methods are used to detect and avoid sinkhole attacks.

1. Existing Approaches

Different peoples are proposed different methods to detect and avoid sinkhole attacks .here we discusses these methods. We consider some previous researchers papers they may be classified into rule based, anomaly based, statistical methods, hybrid systems, cryptographic key management etc *Rule based*: In this approach rules are designed based on the technique or behaviour used to launch attacks (sinkhole attacks). These rules are running on each sensor node. Any node will be considered an isolated and adversary from the sensor network if it attacks the rules. *Anomaly based*: In this method detection and avoid using search the anomalous in the network. Subset of anomaly based detection approaches are Rule based and statistical approaches. Statistical: In this approaches we recorded data associated with some activities of the sensor nodes in network. Then the compromised node is detected by using comparing the correct behaviour of the threshold value the values are used as reference, any seniors node are above that threshold value is considered that nodes are an intruders . *Cryptographic*: In cryptographic approach the dates are protected by using encryption and decryption keys for integrity and authenticity of packets travelling in the whole network. If packets are transmitted in consider network is encrypted the information such that to access the information such that to access the information we requires a key and we can alter the information can be easily detected.

Hybrid: In hybrid method we combine both the combination of both cryptographic approaches and anomaly approach. Benefits of this approach are can able to catch malicious nodes when their signature is not included in detection database and we reduced the false positive rate by using combination of both approaches are transmitted in consider network is encrypted the information such that to access the information we requires a key and we can alter the information can be easily detected.

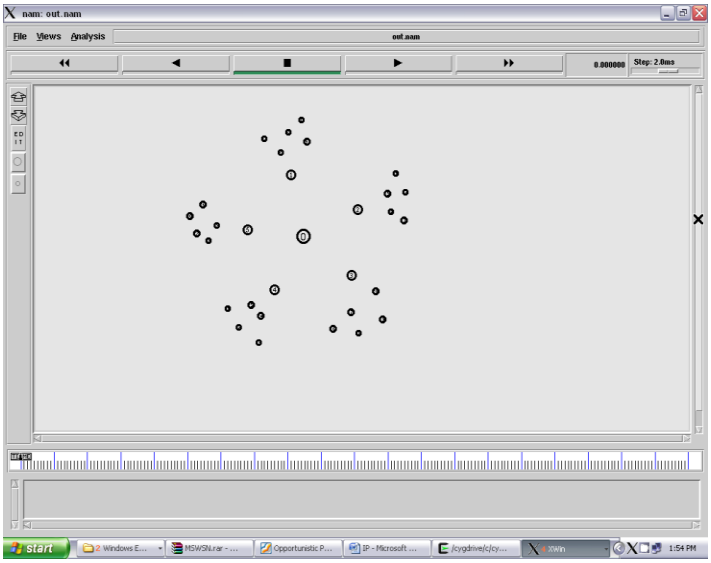
III. PROPOSED SYSTEM

Using one-hop distance nodes are clustered.

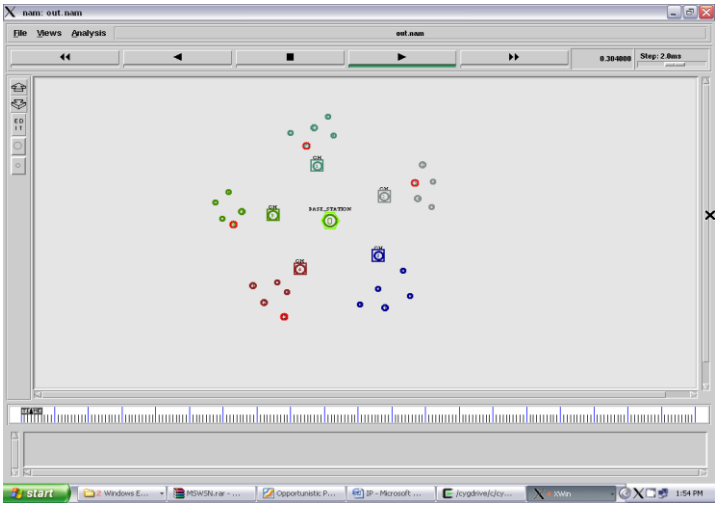
We propose Secure and Efficient data transmission protocols for CWSNs, which achieves security requirements in CWSNs, as well as solved the intruder node problem in the secure transmission protocols. The steps involved in the system as follows:

- IP address of base station is 32 bit.
- There are 'n' of wireless networks, each network contains 'n' number of nodes inside and intruder

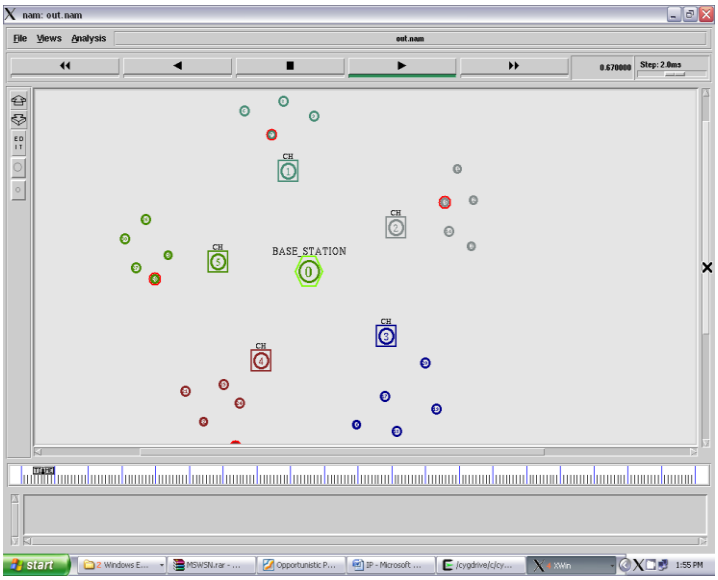
- Each network is controlled by separate 'cluster head'. Cluster head acts as gateway between Network and base station.
- Each cluster head contains 'Access Control List' of that network.
- Access control list contains the Authorized Nodes list in the network.
- Node Access the base station through cluster head .
- Cluster head assigns the IP address of base station by dividing the IP address depending on Number of network
- Suppose if authorized needs to access something from base station means, that is through cluster head only
- Here intruders should not access or steal the address of nodes and also IP address of base station

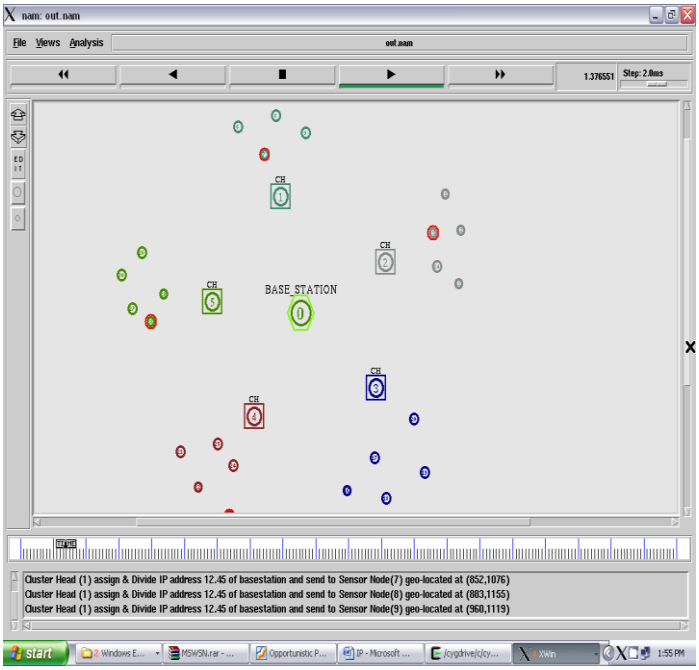


In this figure there is a base station node 0,five cluster heads and each cluster head has 5 nodes.their position is based on the X,Y values for two dimentional representation

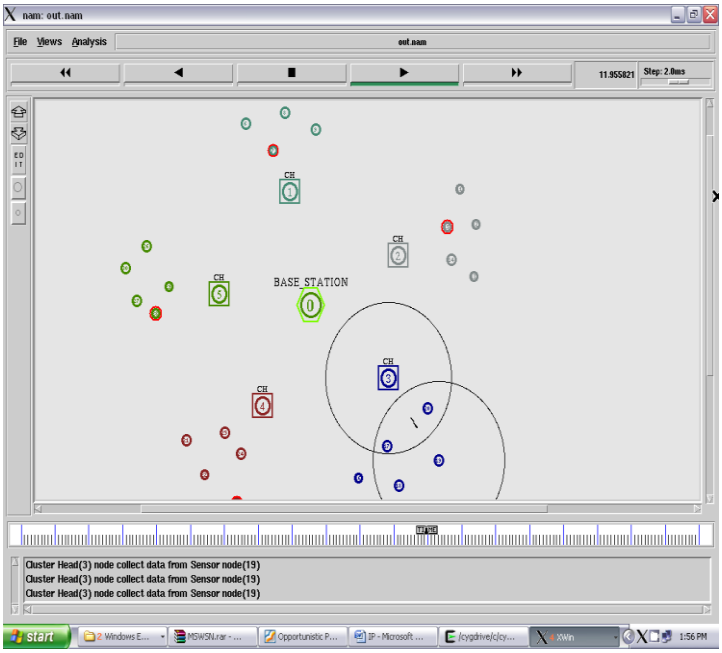


Here base station and cluster heads and their corresponding nodes are represented with some colours.base station has hexagonal shape region,cluster heads with squars and nodes with circles.

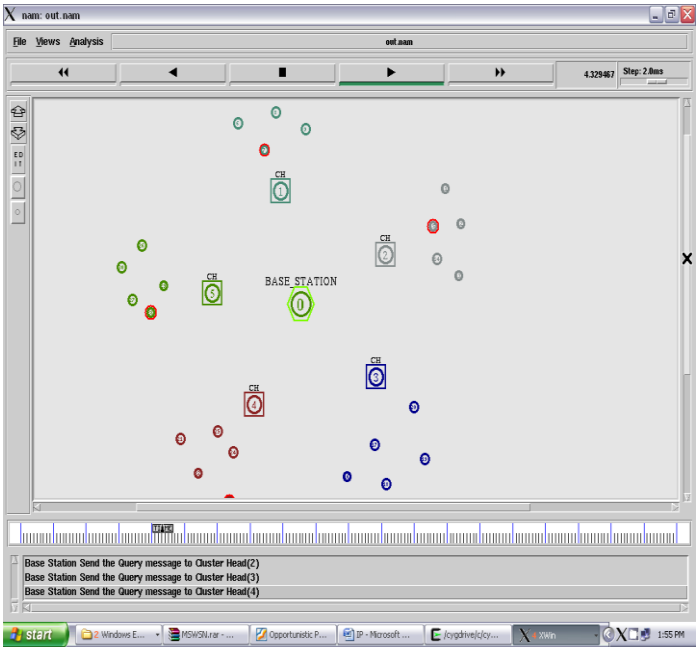




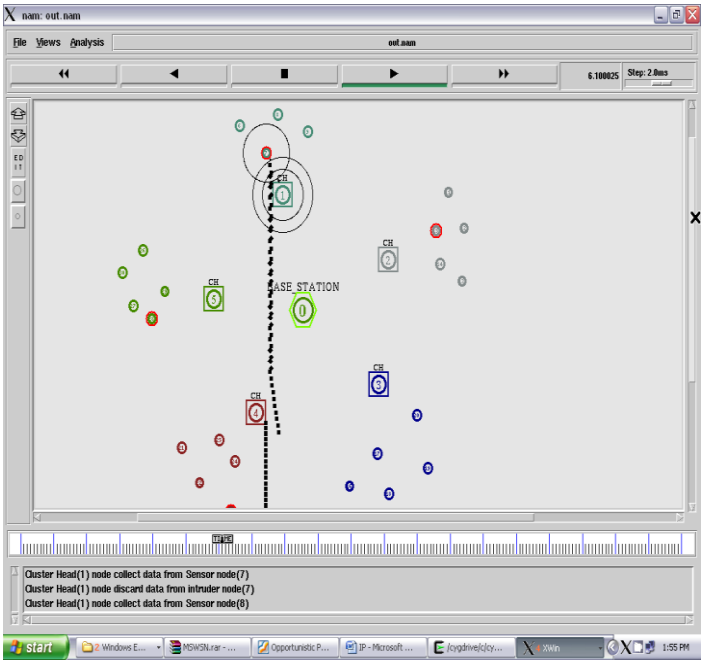
This figure shows how cluster heads assign address to nodes.



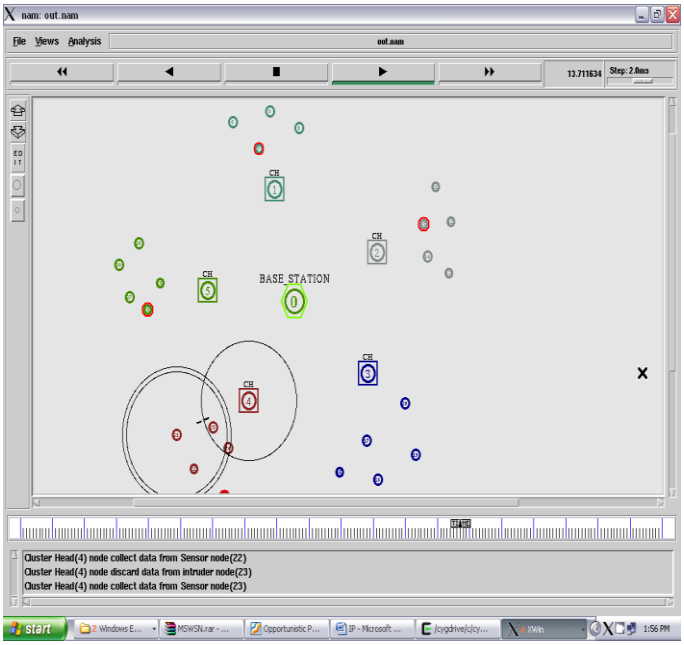
Cluster head node collecting data fron sensor node.



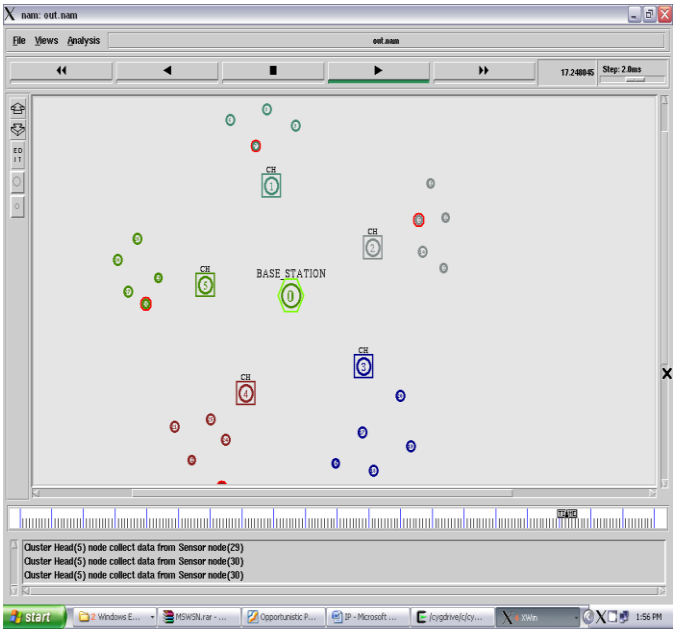
Base station sending query messages to cluster head.

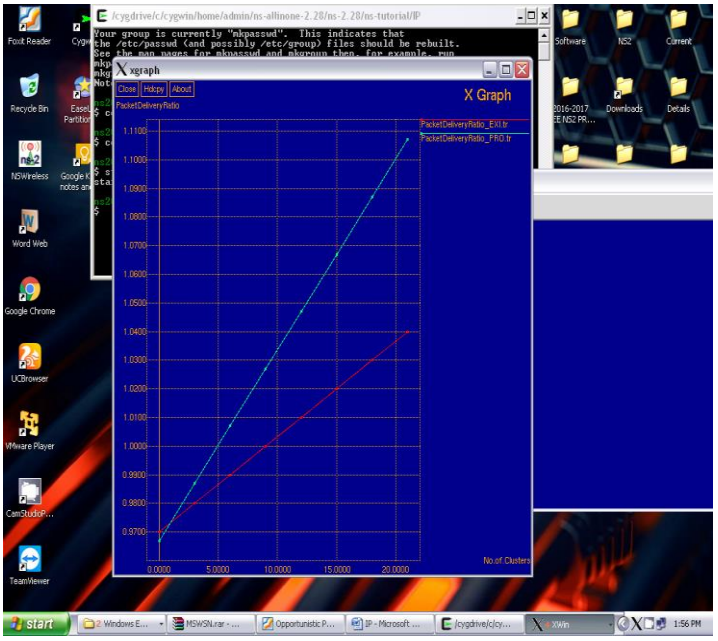


base station collects data from nodes and discards data from intruder.



Same collection and discarding process continues.

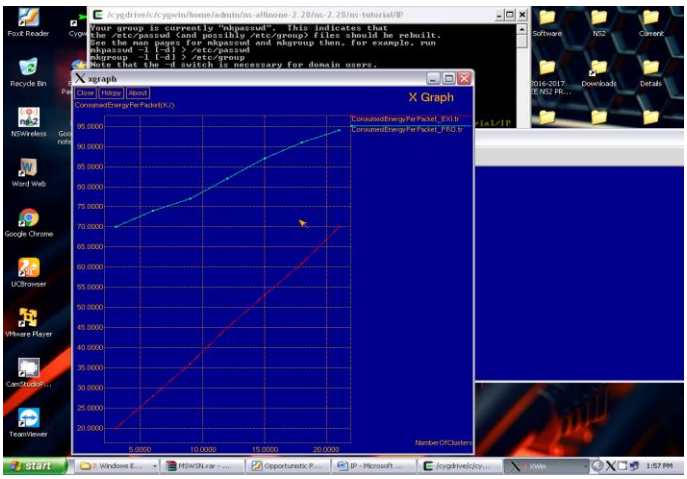




This graph shows comparison of packet delivery ration for existing and proposed system with number of clusters.

This graph shows comparison of delay for existing and proposed system with number of clusters.

This graph shows comparison of lifetime for existing and proposed system with number of clusters.



This graph shows comparison of consumed energy for existing and proposed system with number of clusters.

V.CONCLUSION

Proposed system reduce the possibility of attacking node or introducing malicious nodes in the network with minimum of energy. Because in proposed system the address of Sink node address is divided among the cluster head and there will be Access Control List with every cluster head and it is transferred whenever cluster head changes because of energy constraints.

REFERENCE

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wirelesssensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393– 422, Mar. 2002.

[2] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Communications*

Surveys Tutorials, vol. 15, no. 3, pp. 1238–1280, Mar. 2013.

IEEE Access, vol. 2, pp. 633–651,Jul. 2014.

[4] R. Rios and J. Lopez, "(Un)Suitability of anonymous communication systems to WSN," *IEEE Systems Journal*,vol.7, no. 2, pp. 298–310,Jun. 2013.

[6] A. Proa˜no and L. Lazos, "Perfect contextual information privacy in WSNs under colluding eavesdroppers," .

[7] Y. Ebrahimi and M. Younis, "Using deceptive packets to increase base station anonymity in wireless sensor network," .

[8] V. P. V. Gottumukkala, V. Pandit, H. Li, and D. P. Agrawal, "Base station location anonymity and security technique (BLAST) for wireless sensor networks,".

[9] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *Proc. of the 26th IEEE International Conference on Computer Communications (INFOCOM)*. IEEE,May 2007, pp. 1955–1963.

[10] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks,".

[12] B. Ying, D. Makrakis, and H. T. Mouftah, "A protocol for sink location privacy protection in wireless sensor networks," in *Proc. of the IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, Dec. 2011, pp. 1–5.