Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Defence Scheme to Detect Selective Forwarding Attack in WSN

Harpal Singh*
Department of CSE,PITK (PTU Main Campus),
Kapurthala, India

Vaibhav Pandey
Department of CSE, PITK (PTU Main Campus),
Kapurthala, India

Abstract— Wireless sensor network becomes increasingly popular with the development in technology. It can provide enormous amount of services for the benefit of mankind. But due to its limitations in memory and other resources it is very much prone security attacks, selective forwarding attack is one that security attacks which can affect the whole sensor network communication. The variety of defense scheme has been proposed against selective forwarding attack. In this paper we have propose a defence scheme against selective forwarding attack using info_packet, each node in the forwarding path send info_packet to respective source node after fix interval of time. When source node receive information packet from intermediate node , it identify the malicious node, source node blacklist the malicious and send new route request for communication.

Keywords— Selective Forwarding Attack, Wireless Sensor Network, AODV,

I. INTRODUCTION

In today's world technology is growing at very fast rate each day. Recent advances in digital electronics , wireless communications, and micro-electro-mechanical systems (MEMS) technology enabled us to develop small sized sensor nodes that have a multi-function like sensing, data processing, and wireless communication. These small sized multi-functional nodes can deploy cooperatively to construct wireless sensor network. WSN is emerging as an interesting and promising area. Wsn has proved its utility in number of field in the present world. Wsn is mostly deploying in military field, medical, disaster management and home security systems. Integrated into number of devices, Machines, and environments, sensor provide number of social benefits. They can help to avoid catastrophic infrastructure failures, save precious natural resources, increase productivity, enhance security systems, and enable new applications such as context-aware systems and smart home technologies. But it can be prone to number of security attacks like selective forwarding attack, first proposed by Karlof[1].This type of attack can be very harmful in mission critical application and affect whole communication system. It is very difficult to detect because of its nature, in this attack node work normally but refuse to forward selected packet and drop them or pass to some other sources. Selective forwarding attacks are most harmful when the attacking nodes are explicitly included in the path of data flow . Selective forwarding attack can affect a number of multi-path routing protocols such as Tiny-OS beaconing, directed diffusion, GPSR, and clustering based protocols.

In this paper we propose an efficient lightweight scalable scheme that detects selective forwarding attack using info_packet. Each node in the data forwarding path after fix interval of time send a info_packete to respective source node. Source node receives the info_packet and check to see that packet is directed to it, if not it forward the packet. The source node analyse the info_packet which contain following four fields source node address(src_adrss),packet count(pkt_count),previous hope address(Prev_adrss),destination address(dst_adrss). Source node compare pkt_count field with number of data packet it send on the routing path , if number of packet drop is more than certain threshold source node identify previous node of intermediate node as malicious node ,malicious node will be blacklisted and new route request will be send by the source node to base station.

The remainder of this paper is organised as follows. Section II present the Selective forwarding attack in WSN. In section III related work is described. In section IV , Proposed scheme is described. Section V describe the experimental result and section VI has conclusion.

II. SELECTIVE FORWARDING ATTACK IN WSN

The selective forwarding attack was first introduced by Karloff and Wagner [1]. It is also called as Gray Hole attack Selective forwarding is a denial of service attack which affect the routing data at the network layer[3] , in selective forwarding attack compromised node refuse to forward particular packet on the route to the base station selectively. This attack can be launch by placing malicious node in the routing path which have similar capability of nodes in the network .It can also be launch with the help of sinkhole and wormhole attack. We can categorise selective forwarding attack on the basis of malicious node count in routing path and on the basis of type of packet it drop [2].

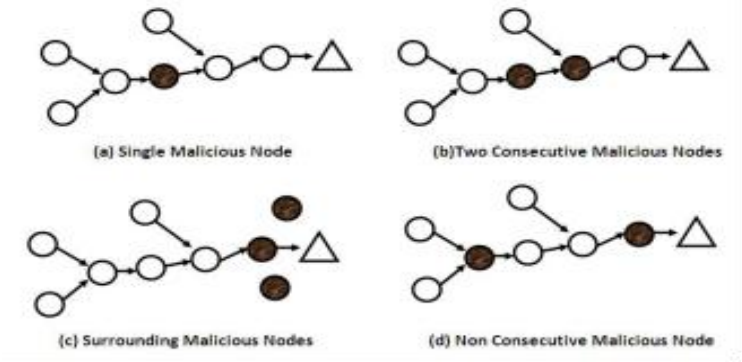

Fig. 1[2] categorization selective forwarding attack based on node count.

Based on the packet it drop selective forwarding attack can be considered into following two types.

1. Drop packet of some specified node.
2. Drop packet of some specified type []

III. RELATED WORK

In this section we review related work on detection of selective forwarding attack. Karloff et.al [1] was first to introduced the selective forwarding attack and also suggest multi-path routing as countermeasures to tackle these type of attacks. According to this scheme, message routed over n path through completely disjoint nodes, it provide some probabilistic protection over n compromised node. It uses multiple braided paths which may provide more protection against selective forwarding attack. In this scheme node probabilistically choose next hop from set of possible candidate, which can further reduced the chance of losing control to adversary. This scheme has poor security resilience, cannot detect malicious node but avoid it.

Xin-sheng et al [4] have proposed a light weight defence scheme against selective forwarding attack. According to this scheme sensor network is divided into hexagonal mesh topology, in each hexagonal there can be only one node is active for the operation. Each node find its geographical location through GPS and find which hexagonal it belong to , node neighbour to this node is set as monitor node which keep close look at each operation of node when any event is occur .The neighbour node monitor the transmission of packet through routing path if any node in routing path drop packet monitor node mark that node as malicious node and change the path of packet to ensure the delivery to the sink. This scheme is very energy efficient as only one node can be activated in each hexagonal cell and also it ensures the proper delivery of data to the base station. There are some limitations of this scheme. This scheme doesn't explain some important aspect. If topology changed scheme cannot perform efficiently, use of GPS make network costly.

K. Sophia et al [5] have proposed a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and have used sliding windows for black hole attacks and selective forwarding attacks. In this particular scheme they only detect the attacks. They also claimed that, this is the first attempt to apply SVMs as a solution in a WSN security. This scheme raises alarm based on the 2D feature vector (bandwidth, hop count) by using routing information local to the base station of the network .Classification of the data patterns is performed using a one-class SVM classifier[5]. They use anomaly detection as base for their scheme. Anomaly detection signals an intrusion when the observed activities differ significantly from those usually undertaken by the user. The authors consider a minimum energy routing protocol, called minimum transmission energy (MTE). Their scheme can detect black hole attacks with 100% accuracy and selective forwarding attacks with 85% accuracy. In this scheme intrusion detection is performed in the base station and hence the sensor nodes use no energy to support this added security feature. Scheme detect malicious node but cannot identify it .

Hea Young et al [6] have proposed a Fuzzy based reliable data delivery scheme to detect the selective forwarding attack which is an improved version of Multi-path routing method. The improvement is that the number of routing path varies with number of attacker. They are both using a redundant strategy such that the event packet is transmitted in multiple paths. Fuzzy logic is used to determine the number of paths for data delivery by considering the energy level of the node in the network and the number of malicious nodes. The proposed scheme uses the propagation limiting method as a means for routing if multi-path routing is insufficient for reliable data delivery. They have also assumed that the base station know or estimate the energy level of network and the number of malicious nodes in advance and that all the nodes know their location. Multi-hop acknowledgement scheme is also used for selective forwarding attack detection.it consume more energy.

Jeremy Brown et.al [7] have proposed a centralised cluster based scheme for detecting the selective forwarding attack in sensor network by using Wald's Sequential Probability Ratio Test(SPRT) method[9].This scheme use powerful high-end sensor and this is bases on the sequential probability ration test .The scheme detect attack with high detection ratio and very low false alarm rate. Each node listens passively for the transmission packet, if any node downstream node drop the packet, the upstream node will observe the packet drop. The monitor node (L-sensor) will send the report packet to cluster head (an H-sensor), the report include the node ID of the dropper. Bases on this report packet, a powerful H-sensor performs the sequential probability ratio test and determines if an L-sensor is compromised or not. Scheme will not work if cluster head is compromised.

Xie lei et al [8] has proposed a polynomial based scheme to detect selective forwarding attack, a security scheme use redundant data to tolerate the loss of critical packets. This scheme split the sensing data into parts and sends these parts instead of the original sensing data to the sink by using a dynamic individual path forwarding mechanism so that, forwarding node cannot understand the contents of the data generated by the polynomial, which can minimise the possibility of eavesdropping. When data reached at sink, it can parse the original event data and if the malicious node tampers with data, sink can detect the tampering of data. There are some assumptions made by the author like the network consists of static sensor nodes and sink having knowledge about topology and it trusted entity in the network and cannot be compromised. Each node in the network shares a unique symmetric key with the trusted sink. If topology changes scheme will not work properly.

Xiao, Yu and Gao [9] have proposed a technique for detecting malicious nodes in selective forwarding attack. They have actually improved their previous technique for detection of selective forwarding attack and named it as CHEMAS (checkpoint-based multi-hop acknowledgement scheme). In this scheme they randomly choose part of intermediate nodes along a forwarding path as checkpoint node. The checkpoint nodes are responsible for generating acknowledgements packet for each event packet received. In addition each node needs a one-way hash key chain for ensuring the authenticity of packets. Delay mechanisms are also developed to send current one-way hash key. Each Intermediate node in a forwarding path has the potential to detect abnormal packet loss and identify suspect nodes if it does not receive enough acknowledgements from the downstream checkpoint nodes. Require more storage space due to us e of one-way hash key, Does not guaranty reliable packet transmission in case of packet dropping.

Hung-Min Sun et al [10] have proposed a multi-dataflow topologies (MDT) method to detect the selective forwarding attack. The authors divide the sensor nodes into two-dataflow topologies by using MDT, both dataflow topology can cover the monitored area, therefore the base station only requires one report from either topology to control the entire network. Through these two topologies the sink can defend against the selective forwarding attack. If a malicious node exists in one topology, the sink can still obtain packets from other topology. To locate a malicious node, the authors deploy the sensor nodes region by region during the deployment phase. Sensor nodes can be located in a range of some regions. When the sink loses some packets, it will mark all possible regions that the malicious sensor nodes may be deployed in. After that, the sink can gather and analyse the information about all possible lost regions; hence the sink can utilize the information to locate the malicious sensor nodes. This Scheme has limited ability to detect malicious node.

Deng et al [11] have proposed a centralized detecting method by watermark using the trust value in the routing selected protocol. They made improvement in the geographic forwarding protocol by combining the trust value with distance to choose an optimal data forwarding path. They use a watermark based scheme is used to detect selective forwarding attack. When attack is detected, detection mode starts. Malicious node can be detected and addressed during this detection mode. Detection accuracy of this scheme is over 95% even with 10% channel error rate. There are some assumptions made by the author like base station is always trusted and cannot be compromised. Each node has trust value which is maintained by the base station. At beginning all nodes in the network has the same trust value and all of trust values change dynamically.Scheme unable to detect more than one malicious node in the routing path.

IV. PROPOSED SCHEME

We would like to mention some assumption and preliminary before explaining about detection scheme.
We make some assumptions which are given following.

1. Selective Forwarding attack only drop data packets.
2. Base station cannot be compromised.
3. Source node has record of number generated packets.

A. Network topology-

We can deploy wireless sensor network by spreading sensor node in deployment field, network can be mobile or static. We consider static topology but our scheme can also perform in mobile sensor network. For routing purpose we used AODV routing protocol. Data packets are being transfer from source to destination through multi-hop routing path.

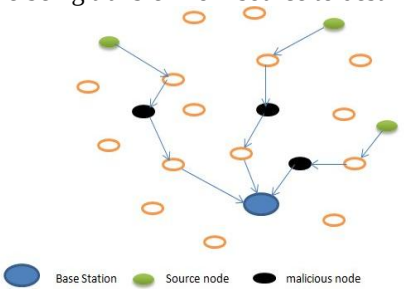

Fig.2 A scenario of selective forwarding attack .

B. Info_packet

Information packet is the packet generated at each intermediate node in the routing path from source to destination .Each node in routing path generate info_packet and send back to source node from which it receive the data packet .structure of info_packet is given below.

Src_adress	Pkt_count	Prev_hope_adress	Desti_adress

Info_Packet

Src_adress:-The address of source node which generate the data packet.
Pkt_count:-Number of packet receives by the intermediate node.
Prev_hop_adress:- Address of previous hop of intermediate node which send info_packet.
Desti_adress;- Address of base station to which packets are directed.

We propose detection scheme to detect selective forwarding attack which work in two phases. In first phase source node send data packet to base station through multi-hop routing path .Each node in the routing path send a info_packet to source node after fix interval of time.In second phase source node receive info_packet and identify the malicious node and send new route request to base station.

I. Phase one: send info_packet routine.
When any source node generates an event and send data packet to sink through multi-hop path. Each intermediate send info_packet to respective source node.

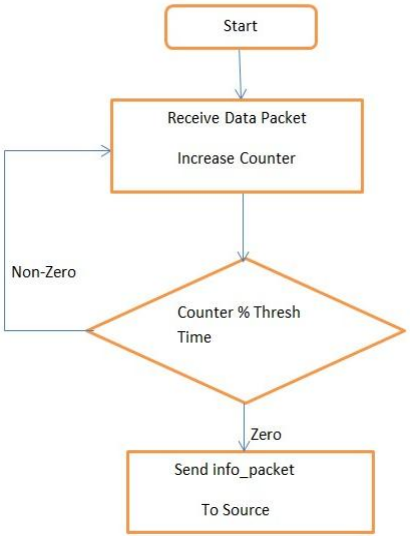

Fig. 3 Flow Chart for Send info_packet routine.

II. Phase Two: Receive info_packet and malicious node identification routine.
In this phase source node receive info_packet and check src_adrsss to see that if info_packet is send to it , if not forward the packet .If packet send for respective source node it compare packet receive by the intermediate node with number of packet it generated. If percentage of packet dropping greater than certain threshold value ,source node mark the previous node of intermediate node which send info_packet as malicious node ,once the malicious node identified it is blacklisted by source node and new route request is send to base station. Flow chart for Receive info_packet and malicious node identification routine is given ahead.

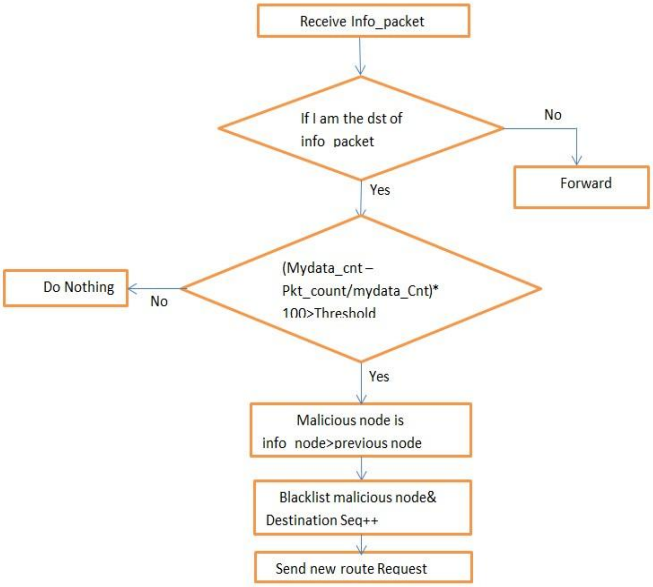

Fig. 4 Flow chart for Receive info_packet and malicious node identification routine

We note the following feature of the proposed algorithm.

- Detection and blacklisting of malicious node is done by source node hence no overload is given to base station.
- Proposed scheme can identify more than one compromised node in the routing path source to destination
- Proposed Scheme blacklist the malicious node so that it cannot included in routing path again.
- Proposed Scheme provide alternative path for data retransmission by sending new route request to base station.

V. EXPERIMENTAL RESULT

The simulation is performed using NS2 Simulation tool. In this simulation network configuration are as follow: The area coverage is 1000 sq meter, 50 sensor nodes are deploy randomly in this area. There is Base station, source node in the network. We place two malicious nodes in the network, other nodes are legitimate nodes.

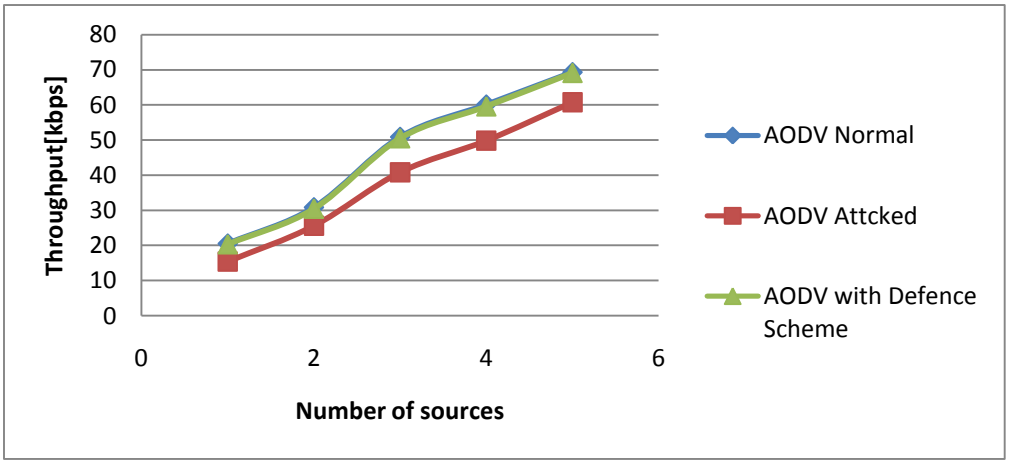

Fig. 5 Throughput v/s number of sources

Throughput table

Number of sources	AODV Normal	AODV Attacked	AODV with Defence Scheme
1	20.5	15.39	20.33
2	30.83	25.58	30.46
3	50.89	40.81	50.52
4	60.1	49.84	59.6
5	69.33	60.74	69.13

In fig. 5 we can see that throughput for normal AODV decrease drastically once it goes under selective forwarding attack .Proposed scheme successfully increase the throughput of AODV. It is seen from figure that performance of AODV increases when we implement the defence mechanism with attacked AODV protocol.

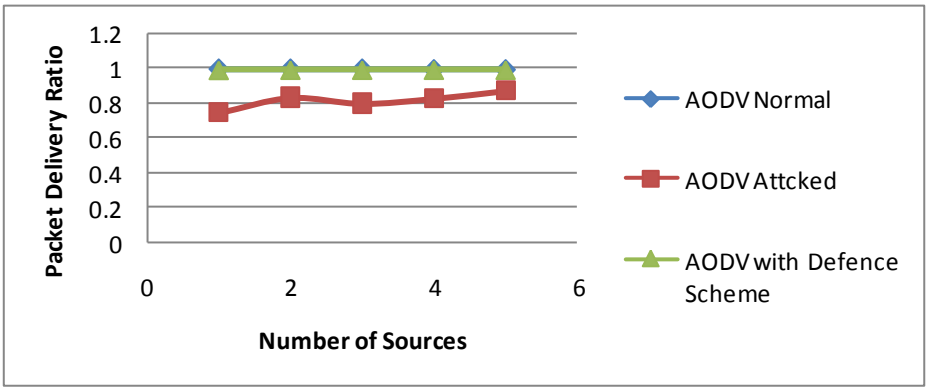

Fig. 6 Packet delivery Ratio v/s number of sources

Packet delivery Ratio table

Number of sources	AODV Normal	AODV Attacked	AODV with Defence Scheme
1	1	0.75	0.9919
2	1	0.8331	0.9932
3	1	0.8006	0.9931
4	0.9962	0.828	0.9931
5	0.9961	0.8712	0.9934

In fig 6 we compare packet delivery ratio for normal AODV, under attack AODV, and AODV with defence mechanism with number of sources. As number sources increases packet delivery ratio decreases for each individual case. Packet delivery of attacked AODV is much lower than that of normal one; our defence mechanism improves the packet delivery ration nearly 95%.

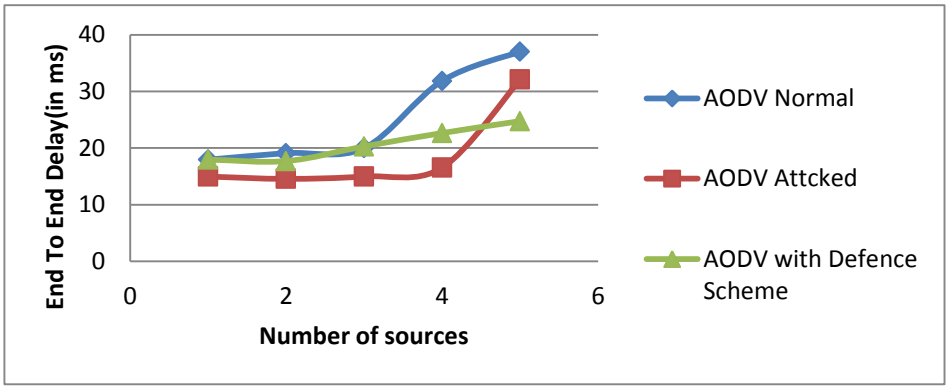

Fig.7 End to end delay v/s number of sources

End to End Delay table

Number of sources	AODV Normal	AODV Attacked	AODV with Defence Scheme
1	17.9456	14.9619	17.9565
2	19.1033	14.5582	17.6989
3	19.9938	14.982	20.2793
4	31.8473	16.5219	22.6459
5	37.0028	32.0954	24.7465

As seen from fig. 7 End to End delay of proposed mechanism comes out to be less than that of normal AODV. Our proposed Mechanism improves the end to end delay in attacked AODV to great extent. But As the number of sources increases the end to end delay also increases and decreases the performance of network, because wireless sensor network has some mission critical application increase in end to end delay may degrade the performance of these applications.

VI. CONCLUSION

This paper propose a method to detect selective forwarding attack in wireless sensor network using info_packet ,each intermediate node send info_packet to source node .The source node will determine whether there is malicious node in the routing path by analysing the info_packet and calculating the packet loss rate by comparing the packet received by intermediate node and packet generated by source node. The detection is done source node and no extra burden is given to the base station. Proposed scheme also suggest alternate path for data transmission by sending new route request to base stations

ACKNOWLEDGMENT

The author wish to acknowledge the anonymous reviewer for valuable comments

REFERENCES

[1] [1] C.Karlof and D.Wagner, "*Secure routing in wireless sensor Networks: attacks and countermeasures*", in Ad Hoc Networks, Vol.1, No.2, 2003, pp.293-315.

[2] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks. Oct.2007.

[3] Harpal Singh, Vaibhav Pandey, "Survey: Detection schemes Against Selective Forwarding Attack" in International Journal of Science and Research (IJSR), ISSN: 2319-7064.

[4] Wang Xin-sheng, Zhan Yong-zhao, Xiong shu-ming, Wang Liangmin, "Lightweight Defense Scheme against selective forwarding Attacks in Wireless sensor Networks" pp.226-232, IEEE, 2009.

[5] S.Kaplantzis,A. Shilton,N.Mani and Y. Sekercioglu, "Detecting Selective forwarding attack in Wireless Sensor Networks Using Support Vector Machines" in 3rd Conf. of Intelligent Sensor Networks and Information Processing,Dec.2007,pp.335-340.

[6] [6] Hae Young, Tae Ho C.Fuzzy-Based reliable data delivery for countering Selective forwarding attack in Sensor Networks. Hong Kong, China, Springer-Verlag, 2007, p.535-544.

[7] J.Brown and X. Du, "Detection of Selective forwarding attack in heterogeneous sensor networks", in International Conf. on Communications, May 2008,pp.1583-1587.

[8] Xie Lei, Xu Yong-Jun, Pan Yong, Zhu Yue-Feil, ,"A Polynomial based Countermeasures to Selective Forwarding Attack in WSNs"International Conference on Communications and Mobile *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[9] B.Yu and B.Xiao, "CHEMAS: identify suspect nodes in Selective forwarding attacks "in Journal of Parallel and Distributed Computing, Vol.67, No.11, 2007, pp. 1218-1230A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[10] H.Sun, C.Chen and Y.Hsiao, "An efficient Countermeasures to the selective forwarding attack in wireless sensor Networks", in IEEE TENCON 2007, Oct.2007, pp.1-4

[11] Deng-yin,Chao,Lin Siyuan, "Selective forwarding attack Detection using Watermark in WSNs"International Colloquium on Computing ,Communication, Control, and Management(2009 ISECS),pp.109-113,2009,pp.445-459.

