2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India

Dynamic Sequence Number Thresholding Protocol for Detection of Blackhole attack in Wireless Sensor Network

Abhijeet Salunke
Sardar Patel Institute of Technology
Andheri, India
Email: abhijeet_salunke@ymail.com

Dayanand Ambawade
Sardar Patel Institute of Technology
Andheri, India
Email: dd_ambawade@spit.ac.in

***Abstract*—The Wireless Sensor Network (WSN) is a distributed wireless micro-electronic-mechanical system which is deployed in hostile environment, has inherent insecure communication medium and resource constraints. This makes security of Wireless Sensor Network challenging. The blackhole attack is a security threat which manipulates sequence number to degrade the performance of the WSN by increasing packet loss. In this research we present a protocol that detects manipulation of sequence number and thus secures network from blackhole attack by sequence number thresholding. The significance of protocol is unlike other methods this thresholding is dynamic and carried out in real time.**

I. Introduction

The wireless sensor network have found their way in many sectors including healthcare, automobile , flit management, military applications and many more. Due to its small size, inexpensive nature and robustness it could be deployed in hostile environment such as battlefield or nuclear reactors [1]. Being small and wireless adds a restriction on hardware support causing resource constrains such computational power, memory and energy [2] [3]. WSN perform many monitoring and tracking work as well as assist many smart tasks [4]. The lifespan of a sensor network depends upon the battery life of individual sensor nodes. The wireless sensor network makes use of air as communication medium. These characteristics of wireless sensor network make it more vulnerable to security threats.

The blackhole attack is one of the well known security threat that exploits wireless sensor network. The blackhole node increases the packet loss of the network [5]. In this attack blackhole node make itself appear more attractive [5] [6]. Hence, most of the nodes in the network route their packets through the blackhole node to sink node. After route establishment Blackhole node starts dropping data packets coming from other nodes causing packet loss of the network to increase [7]. To make itself more attractive blackhole node commonly make use of maximum or very large sequence number in the reply [8] [9]. This suggests that blackhole node has most fresh route towards the sink node. So, if method is able to detect the malicious manipulation in sequence number it can detect blackhole node in the network. For this reason a protocol is presented in this paper to detect manipulation in sequence number by dynamic sequence number thresholding which will result in detection of blackhole nodes in the network.

The rest of the paper is organized as section 2 contains Literature Review. Section 3 consists of Proposed Protocol.Section 4 contains Experimental Setup along with section 5 and 6 which consists Results and Conclusion followed by References.

II. Literature Survey

Different literatures are reviewed in order to deduce the flaw in existing system against blackhole attack making use of sequence number as criteria. After reviewing many literatures two prominent works based on sequence number in domain of security were deduced. In Literature [8] the protocol considers only first entry in the routing table for any sequence number manipulation. This is based on the assumption that a blackhole node sends the reply as soon as it receives a request from neighboring node. Hence delay is less compared to other reply packets making the entry of malicious node the first among routing table. But this cannot be true many times especially for complex networks and so, this idea fells short for catering large set of blackhole attacks.

In Literature [9] the protocol establishes a threshold range of maximum sequence number and uses it as to detect manipulation. In the worst case this threshold is about 94% of maximum sequence number (i.e. 4294967296) in wireless sensor network route discovery packet which is a 32-bit number. The attackers now a day are smarter and thus use a sequence number considering size of the network. This sequence number is large enough to affect the performance of the network but not as large as 94% of maximum 32 bit sequence number. And thus the protocol suggest by literature 2 do not attain smartly implemented blackhole attacks.

Due to this drawback in existing methods a new improved protocol which deals with blackhole attack is needed. This drawback of present system drives need for this research.

III. Proposed Protocol

The proposed protocol discussed in this section is Dynamic Sequence Number Thresholding (DSNT) Protocol for securing network against blackhole attack. For detecting the blackhole attack we use its large out of bound sequence number as a signature. We put a threshold on the sequence number from the RREP packet that is reply packet. Here, RREP is a feedback

978-1-4799-5522-0/15/$31.00

message and sequence number decides whether it is benevolent or malicious. The threshold for sequence number 'S_h' is calculated as in Equation 1. To implement the DSNT protocol we modify AODV routing protocol. We add a new column named node grade into the routing table which represents whether a node is benevolent (B) or malicious (M). The Figure 1 represents the flow of DSNT protocol.

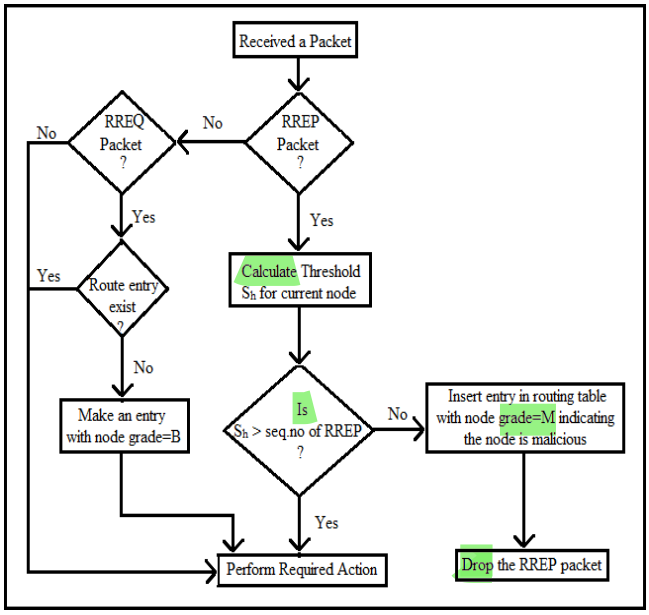

Fig. 1. Process Flow of Dynamic Sequence Number Thresholding Protocol

$$S_h = \lambda * N + maxof(seqno) \quad (1)$$

Here, 'N' refers to number of nodes in network and '*maxof(seqno)*' refers to the maximum of sequence number from route table entry of current node routing the packet excluding malicious node entries. The 'λ' is Sequence Number Increment Constant which represents amount of sequence numbers generated, that is packets routed, in the network in worst case scenario. The threshold calculation for S_h must be done from the maximum of sequence number in the route table of the current routing node. In addition the size of network must be consider in this calculation as for larger network, the sequence number will be generated at much faster rate as more number of node would want to send data to sink. Therefore at the worst case during the route discovery of a node, we may assume that all the nodes in network generated a RREQ and RREP packet increasing the sequence number [10]. Hence 2 times the number of nodes in network is added in the max(seqno). This brings λ value to 2. The value of λ may be fine tuned for different networks depending upon communication overhead and topology of the network. Hence Equation 1 is now reduced to Equation 2.

$$S_h = 2 * N + maxof(seqno) \quad (2)$$

The flow of the DSNT protocol is represented by Figure 1. When RREQ packet is initiated by any node for route discovery, the route entry along with node grade value as benevolent by default is inserted into every nodes route table about the previous node from which it receives RREQ packet. If route entry already exists it is updated. When black hole node receives this packet it sends a RREP reply packet to its source with manipulated large sequence number. When node running DSNT protocol receives a RREP packet it checks packets sequence number against sequence number threshold S_h. If sequence number of RREP if lesser that threshold S_h then packet is accepted and required further processing is done. Otherwise the node grade of node from which RREP is received is changed to malicious 'M' then RREP packet is dropped.

IV. Experimental Setup

The simulation is performed in NS-2.35. Parameters of the simulation are shown in Table I.

Parameter	Value
Propagation Model	TwoRayGround
Network Interface	802.15.4
Queue	DropTail
Antenna	OmniAntenna
Queue Length	50
Number of Nodes	25
Area	50*50
Routing	AODV
Initial Energy	1000 Joule
Idle Power	712e-6 Watt
Transmission Power	31.32e-3 Watt
Reception Power	35.28e-3 Watt
Sleep Power	144e-9 Watt

TABLE I. Parameter for Simulation of Wireless Sensor Network.

The simulation is performed for scenario of AODV without Blackhole node. Basically this scenario is generated to show how AODV works normally in the absence of blackhole attack. This helps us to understand change in the routing behavior when DSNT protocol is implemented as remedy against black-hole attack. This helps us to calculate the effectiveness of the DSNT protocol in the event of blackhole attack in forthcoming section. In the Figure 2 flow between node 19 and sink node 0 is very important as further discussion would be done based on the route taken between these two nodes.

As seen from Figure 2 the node 19 forwards its packets to node 14 which intern forwards this packet to node 23 which in the end sends packet to sink node 0. So, the route between node 19 to sink node 0 is node 19 $\Rightarrow$ node 14 $\Rightarrow$ node 23 $\Rightarrow$ sink node 0.This is the normal route deduce by AODV when blackhole is absent. The route table of node 19 is shown in Figure 3.

The routing table shows the routing information needed by all the packets to route through WSN. The entry in each row of routing table is destined to the node represented by column Destination. Now we will see the behavioral changes in routing mechanism when DSNT protocol is implemented.

V. Simulation and Results

This is a decisive section which decides the usability of DSNT protocol against blackhole attack. The topology is same

978-1-4799-5522-0/15/$31.00 ©2015 IEEE

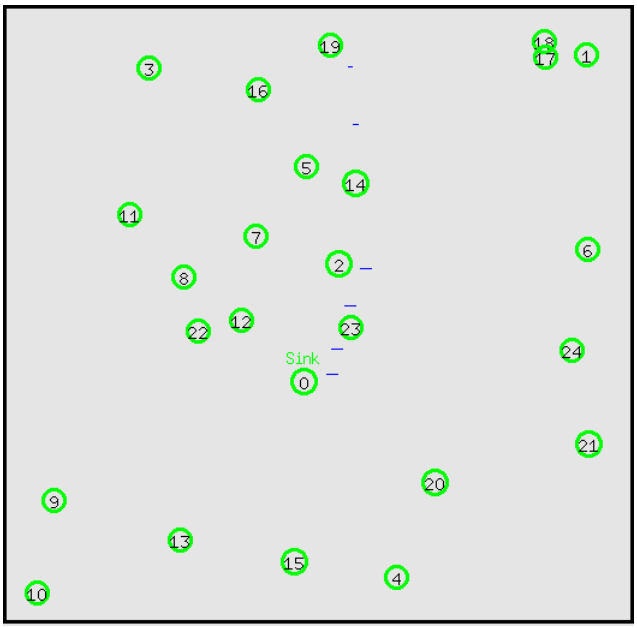

Fig. 2. Routing between node 19 to 0 (AODV without Blackhole node).

```
 GNU nano 2.2.6                File: node_19

Node Id:19 Current time:61.4189 Source:3 Seq. No.:25 Route expire:0.000000 Flags:0.0000
Node Id:19 Current time:61.4189 Source:0 Seq. No.:7 Route expire:0.000000 Flags:0.0000
```

Fig. 3. Routing table of node 19 (AODV without Blackhole node).

as previous section but in this scenario node 14 act as a blackhole node, that is malicious node. From earlier section we know that node 14 is on the route from node 19 to sink node 0 when there is no blackhole node. But now node 14, that is one of the node on the route between node 19 to sink node 0, act as malicious blackhole node. Hence, if DSNT can avoid node 14 while routing it implies that DSNT protocol provides security against blackhole node. The route taken by packets between node 19 and sink node 0 is shown in Figure 4.

From the Figure 4 the route taken by packets is node 19 $\Rightarrow$ node 5 $\Rightarrow$ node 2 $\Rightarrow$ sink node 0. This shows that DSNT protocol avoids the malicious blackhole node, which is node 14. Hence, DSNT protocol provides security aware routing. Now let us see the routing table of node 19 shown in Figure 5.

When node 19 receives a RREP packet from node 14 with a sequence number which do not satisfy sequence threshold S_h, it marks it as malicious by assigning node grade value as 'M' as can be seen from Figure 5. Thus node 19 selects other alternative available node, which is node 5, to route the packets.

In Figure 6 'Green' bar represents packet delivery ratio of AODV protocol without presence of blackhole node in network, 'Red' bar represents packet delivery ratio of AODV protocol in the presence of blackhole node and 'Yellow' bar represents packet delivery ratio of DSNT in the presence on blackhole node.

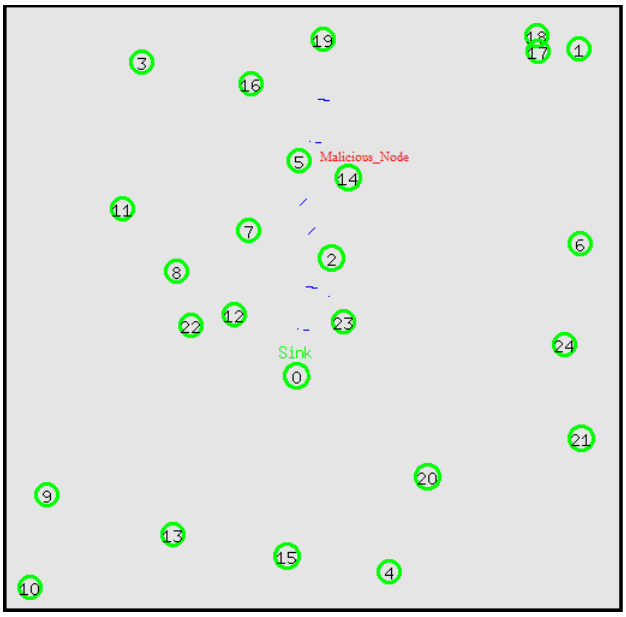

Fig. 4. Routing between node 19 to 0(DSNT with Blackhole node(node 14)).

```
 GNU nano 2.2.6          File: node_19                    Modified

Node Id:19 Current time:95.6891 Source:3 Node grade:B Seq. No.:44
Node Id:19 Current time:95.6891 Source:14 Node grade:M Seq. No.:111431
Node Id:19 Current time:95.6891 source:5 Node grade:B Seq. No.:237
```

Fig. 5. Routing table of node 19(DSNT with Blackhole node(node 14)).

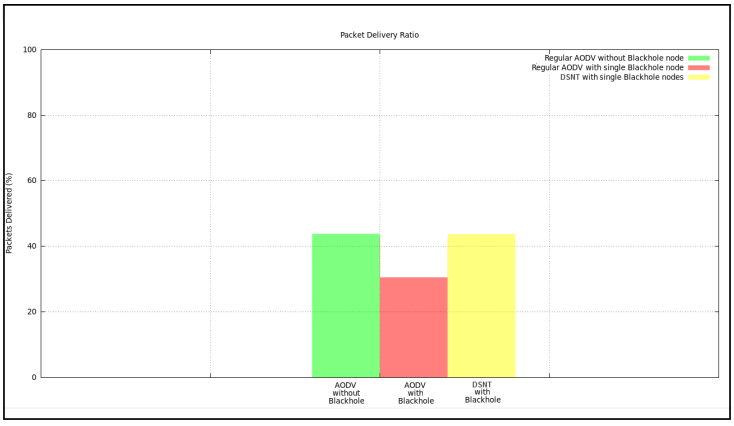

Fig. 6. Packet Delivery Ratio

- Packet Delivery Ratio of AODV protocol without Blackhole node = 43.79 %
- Packet Delivery Ratio of AODV protocol with Blackhole node = 30.13 %
- Packet Delivery Ratio of DSNT protocol with Blackhole node = 43.79 %

From the Figure 6 it is clear that packet delivery ratio of AODV decreases to 30.13% due to the presence of blackhole attack. But when DSNT protocol is implemented within the network for same scenario, the packet delivery ratio of DSNT protocol in the presence of blackhole attack is 43.79%, which

978-1-4799-5522-0/15/$31.00 ©2015 IEEE

is equal to the packet delivery ratio of AODV protocol in the absence of blackhole attack. This proves that packet loss due to blackhole node is avoided by DSNT protocol in the WSN.

This scenario proves that DSNT protocol provides security against blackhole attack in WSN. It can even secure WSN in the event of multiple blackhole nodes.

VI. Conclusion And Future Scope

The results discussed in previous section prove that Dynamic Sequence Number Thresholding protocol detects the blackhole node in the network. The DSNT protocol protects the network against blackhole attack and maintains the packet delivery ratio intact. The blackhole node is marked with node grade value as 'M', so that node could be blocked and won't degrade network performance. In the similar manner DSNT protocol also provide security in the event of multiple blackhole nodes.

Thus DSNT protocol achieves its goal to provide security from blackhole attack which exploits sequence number to launch an attack on wireless sensor network.

Fine tuning value of λ serves as future scope of this research. The value of the λ can be made network specific depending upon the context of different wireless sensor networks. That means value of λ can be tuned to fulfill the requirement of once specific network only. This work needs a more detailed study of message exchange taking place in that specific network for which fine tuning of λ is carried out.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, 'Wireless sensor networks: a survey', *Elsevier Computer Networks*, vol. 38, pp. 393-422, 2002.

[2] Xiangqian Chen, Kia Makki, Kang Yen and Niki Pissinou, 'Sensor Network Security: A Survey', *IEEE Communication Survey & Tutorials*, vol. 11, no. 2, pp. 52-73, Second Quarter, 2009.

[3] Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu and Nael Abu-Ghazaleh, 'An Application-Driven Perspective on Wireless Sensor Network Security', *ACM International Workshop on QoS and Security in Wireless Networks*, Torremolinos, Malaga, Spain, 2 october 2006.

[4] Yan Yu and Yubao Yao, 'Improved AODV Routing Protocol for Wireless Sensor Networks and Implementation Using OPNET', *IEEE Third International Conference on Intelligent Control and Information Processing*, Dalian, China, pp. 709-713, 15-17 July 2012.

[5] Bala, Anu , Bansal M. and Singh J. , 'Performance Analysis of MANET under Blackhole Attack', *IEEE First International Conference on Networks and Communications*, Chennai, India, pp. 141-145, 27-29 Dec 2009.

[6] Rohit Tiwari and Monika Kohli, 'Security Aspects for Wireless Sensor Network', *International Journal of Engineering Research & Technology*, vol. 1, no.8 , pp. 1-7, October 2012.

[7] Abhishek Pandey and R.C. Tripathi, 'A Survey on Wireless Sensor Networks Security', *International Journal of Computer Applications* , vol. 3, pp. 43-49, June 2010.

[8] K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama, K. Thilagam,'Modified AODV Protocol against Blackhole Attacks in MANET', *International Journal of Engineering and Technology*, Vol.2 (6), pp. 444-449,2010.

[9] Seryvuth Tan, Keecheon Kim,'Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs', *IEEE International Conference on Telecommunication* , pp. 1027-1032,2013.

[10] Waltenegus Dargie and Christian Poellabauer, 'Network Layer' in *Fundamental of Wireless Sensor Network Theory and Practices*,1^{st} Edition, Wiley Publication, UK, chap. 7, pp. 163-203, 2010.

978-1-4799-5522-0/15/$31.00 ©2015 IEEE