Vampire attack Detection and Prevention using DLWASN on Wireless Adhoc Sensor Network

Ms. Priyanka P. Pawar. M.E.I.T [2] | Prof. shailaja N. Uke

[1](Department of Information Technology, SKNCOE, Pune, India, Priyapawar2009@gmail.com)
[2](Department of Information Technology, SKNCOE, Pune, India, snuke@sinhgad.edu)

Abstract— *Wireless sensor network (WSN) is very popular research area now days. WSN mainly used in industrial and consumer applications like heath care monitoring and machine health monitoring. Major challenge in front of WSN is security. There are many attacks on wireless sensor network which make network vulnerable. Vampire attack is one of the newly introduced attacks on wireless sensor network. There are two types of vampire attacks first is stretch attack and another is carousel attack. In stretch attack malicious node purposely choose longest route for packet forwarding. In carousel attack packet moves in loop. Stretch attack is difficult to detect than carousel attack. These attacks are routing attacks. The basic purpose of these attacks is to drain the energy of available nodes in the network. There are many detection and protection mechanisms are available but nothing is very specific. The paper discussed about how DLWASN routing protocol scheme is better than beacon routing and clean slate routing with implementation and results.*

Keywords— WSN, Vampires attack, DLWASN

1. INTRODUCTION

Vampire attack:

Vampire attack is characterized as the arrangement and transmission of a message that causes more vitality to be devoured by the system than if a genuine hub transmitted a message of indistinguishable size to the same goal, albeit utilizing distinctive packet headers.

There are two types of vampire attack.

A. Carousel attack:

The noxious hub orchestrates bundles with intentionally presented directing circles. In light of restricted check of parcel header at sending hubs, it permits a private bundle

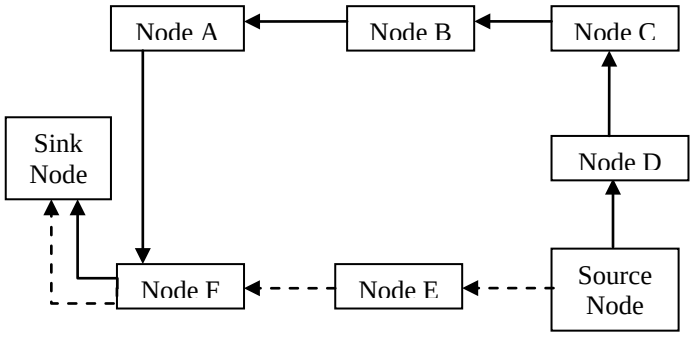

Fig. 1.Caurosel attack

to more than once navigate the same set of hubs. Fig. 1 shows a representation of carousel attack. Source node transmits a packet to sink. The required path is Source-E-F-Sink. But malicious node moves the packet to Source-D-C-B-A-F-Sink. In between D-C-B-A-F-E path repeated 2-3 times. The transmitted packet moves in loop for no. of times. It causes energy drain.

B. Stretch attack:

The malicious node purposely creates long routes, probable traversing every node in the network. Fig. 2 shows stretch attack. The valid route from source to sink is **source-E-F-sink**, but malicious node chooses the longest route like **source-D-C-B-A-F-Sink**. Stretch attack is difficult to detect.

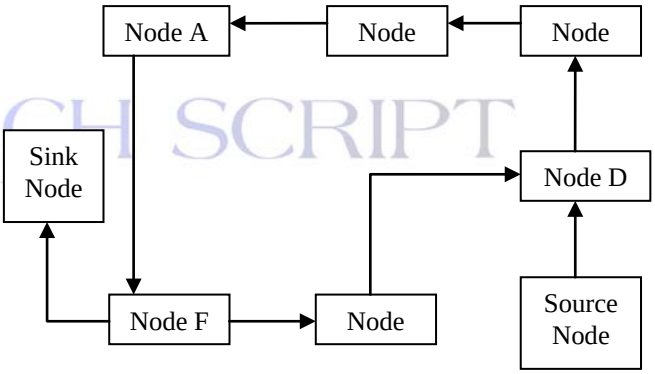

Fig. 2. Stretch attack

2. DLWASN

Protocols given in [3] [6] [8] are vulnerable to detect vampire attacks. These protocols are unable to detect vampire attacks in adhoc sensor networks. Paper proposes a new protocol called DLWASN. The protocol follows with node authority. Each node should prove its identity. Secure hash function is used as cryptographic function. Protocol proceeds with further steps.

A. *Security signature:*

Every node must announce its presence by broadcasting certificate of identity including public key. Public key is referred as node ID. SHA [10] is used to sign trusted authority of signature.

B. Group formation:

Every trusted node started self grouping of size one, with virtual address 0. With the same initial address 0,

nodes form a group of one and virtual address will become 0 and 1. Group merges with nearest neighbour, which may be a single node. Each node choose the group address either 0 or 1 when merging with another group and address will become like Node 0 in group 0 become 0.0 and Node 0 in group 1 become 1.0

C. Tree formation:

Each time two groups merge, the address of each node is expanded by one bit. Implicitly, this forms a binary tree of all addresses in the network, with virtual address at leaf node. This tree is not a virtual direction framework, as the main data coded by the tree is neighbour connections among hubs.

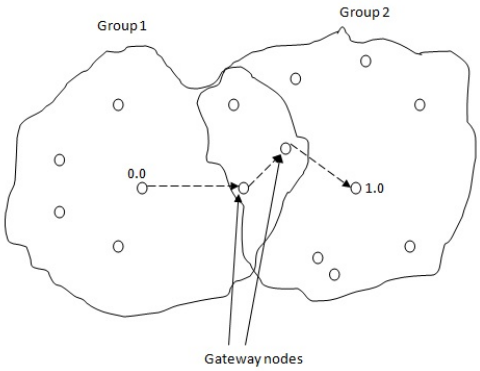

Fig. 3. Gateway node

When larger group merges they broadcast their group IDs and IDs of all group members to each other, and proceed with merging with two nodes. Within large groups some members are not in radio range, communicate via gateway nodes shown in fig. 3. Gateway nodes are within the range of both groups. Every node stores the character of one or more hubs through which it heard a report that an alternate gathering exists. That node may have itself heard the information second-hand, so every node connects the group with address of next hop. Topology disclosure continues in this way until all system hubs are parts of a solitary gathering.

Fig. 4 shows tree formation of nodes which gives parent and child nodes with its virtual address. Leaf nodes are considered as nodes in network. In fig. 4 sender node wants to transmit packet to receiver. It follows address of its neighbour node.

D. Packet forwarding:

All decisions are taken individually by each node. Each node finds the MSB (most significant bit) from address of each node and determines the next hop. Thus every forwarding event within a group shortens the logical distance to the destination, since node addresses should be nearer to the destination. [1]

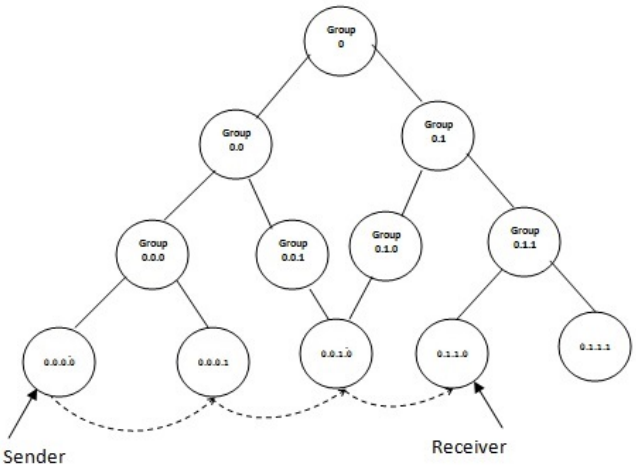

Fig. 4. Tree formation

Honest nodes can show and get messages, while pernicious hubs can likewise utilization directional receiving wires to transmit to (or get from) any hub in the system without being caught by whatever other hub[4]. Legit hubs can make, forward, acknowledge, or drop messages; also noxious hubs can likewise self-declaratively change them. Our malicious node is accepted to control m hubs in an N –node system (with their relating character declarations and other mystery cryptographic material) and has impeccable learning of the system topology. At last, the foe can't influence network between any two genuine nodes.

At the point when any hub gets a message, it watches that each hub in the way verification

1) Has a relating passage in the mark chain [1], and
2) Is legitimately closer to the end of the line than the past bounce in the chain [secure packet forward].

In this way forwarding nodes can impose the forward progress of a message, preserving no-backtracking [1]. If there is no attestation with node then node checks to see if the originator of the message is a physical neighbor. All messages should be signed with sender's signature. Attacker node cannot find origin of message and therefore cannot remove attestation.

3. PERFORMANCE CONSIDERATION

To examine the performance of DLWASN we used NS-2 as simulation tool. Results are plotted using x-graph. Following parameters are considered for simulation given in Table 1.

TABLE I. Network parameters

Network interface type	Wireless physical
Radio Propagation Model	Two-Ray Ground
Channel Type	Wireless Channel
MAC	802.11

Routing Protocol	DLWASN
Total no nodes	100
Link Layer	Link Layer (LL)
Antenna	Directional Antenna
No. of packets to be transmit	1300
Initial Energy	100J

a. Average damage verses packet drop ratio

Fig. 5 shows the graph of average drop verses packet drop. As number of nodes increases packet drop is increases, but as compared to other protocols average damage is less for secure forward.

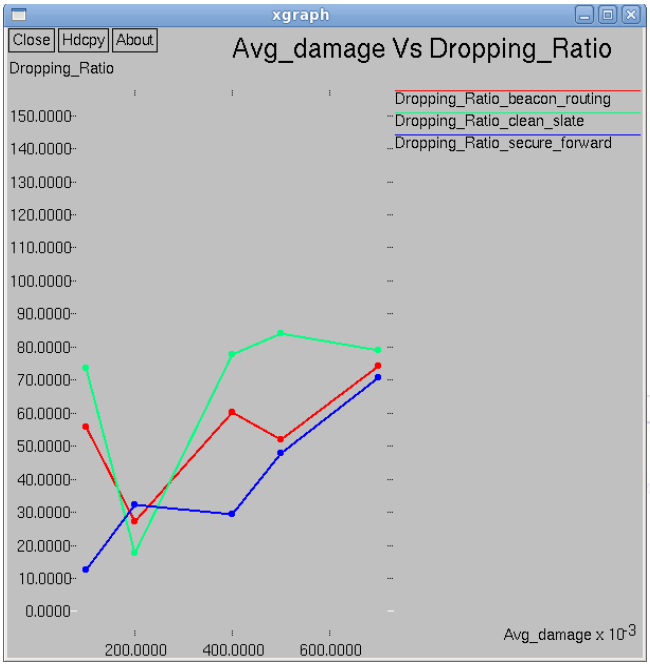

Fig. 5. Average drop verses packet drop

b. Average damage verses Throughput

Fig. 7 shows that secure forward protocol produce better throughput than became routing and clean slate. DLWASN protocol is given more throughput than other protocols.

c. Average damage verses average energy

Fig. 6 shows that secure forward protocol consumes less energy than became routing and clean slate. As number nodes increases energy consumption is more but as compared to other protocols less energy consumption for secure forward.

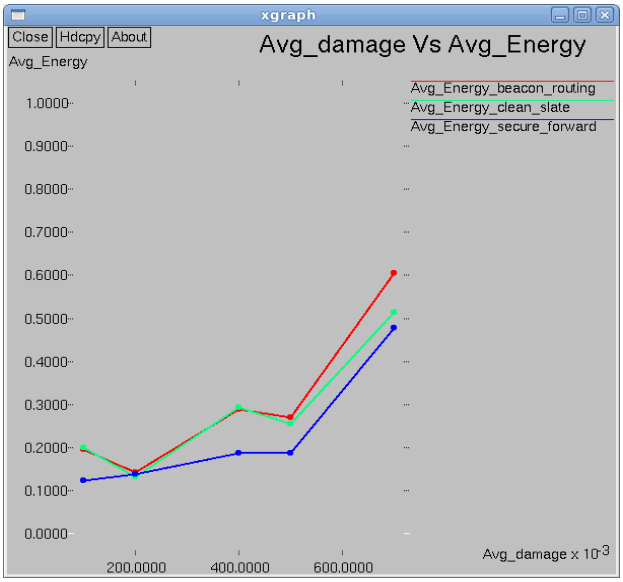

Fig. 6. Average damage verses average energy

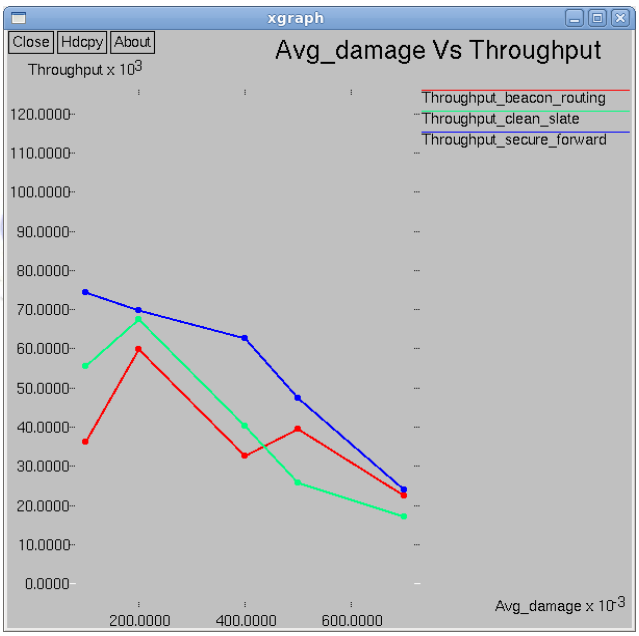

Fig. 7. Average damage verses Throughput

d. Average damage verses delay

Fig. 8 shows that the comparison for required time to transmit packet. Secure forward is taking somewhat similar time like beacon routing.

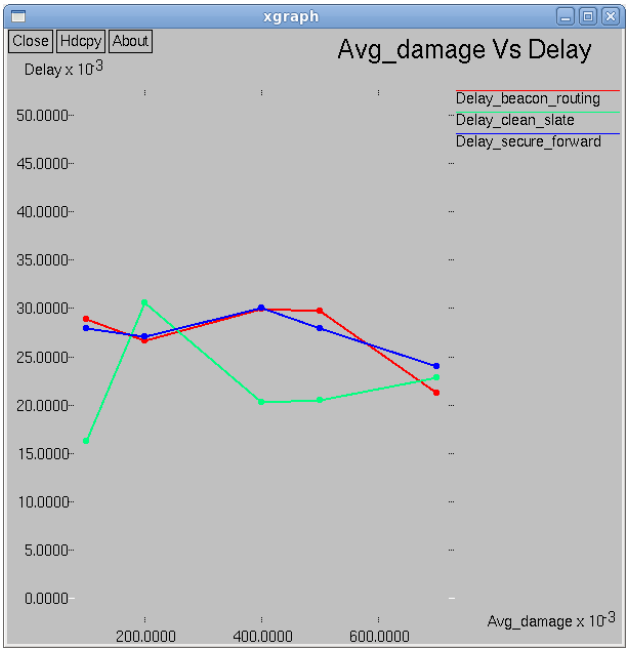

Fig. 8. Average damage verses Delay

4. CONCLUSION

In this paper we proposed new routing protocol called DLWASN. It is better routing than beacon and clean- slate routing. We computed results based on four parameters like PDR, energy, throughput and delay. While considering PDR, Energy consumption and throughput protocol gives better results than others but packet transmission delay is properly maintained in Clean-slate. DLWASN has given better results for some parameters but like delay and other which are not considered may remain for future work.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper, FEBRUARY 2013, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2.

[2] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho, March 2013,"A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks", 33-40, scientific research.

[3] Ivan Stojmenovic and Xu Lin, 2001 "Power aware localized routing in wireless sensor network:" IEEE transaction on parallel and distributed system, vol 12, no 10.

[4] J. Gomez, J. M. Cervantes, V. Rangel and R. Atahualpa, Miguel Lopez-Guerrero, 2007, "NARD: Neighbor-Assisted Route Discovery in Wireless Ad Hoc Networks",IEEE.

[5] Jing Deng, Richard Han, and Shivakant Mishra, *November 7, 2005*, "Defending against Path based DoS Attacks in Wireless Sensor Networks", *SASN'05*.

[6] Sheetalkumar Doshi, Shweta Bhandare_ Timothy X Brown, "An On-demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network.

[7] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan and Xiaole Bai, "Providing End-to-end Secure Communications in Wireless Sensor Networks".

[8] YIH-CHUN HU and ADRIAN PERRIG and DAVID B. JOHNSON, 2005, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks 11, 21–38, ,Springer Science + Business Media, Inc. Manufactured in The Netherlands.

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE INFOCOM 2003.

[10] http://en.wikipedia.org/wiki/Secure_Hash_Algorithm