# Secure Transmission against Vampire Attack using Wireless Adhoc Sensor Network

Shubhangi Pokharkar
MBES College of Engineering,
P.G. Dept,
Ambajogai, India, 4315 17

Veeresh G. Kasabegoudar
P.G.Dept,
MBES College of Engineering,
Ambajogai, India, 431517

## ABSTRACT

Adhoc wireless networks are interest among the researches in sensing and ubiquitous computing. The security focused especially on denial of communication at the routing or transmission of data using protocol. Vampire attacks are stubborn to detect, disastrous and are easy to carry out using as few as one network wide energy usage. These affect on OS and suddenly break the function. Therefore to oppose this situation, in this paper a secure transmission method proposed which will protect the system and alternative protocols solutions that will be avoiding some sort of problems which are caused by vampire attack. This technique transfers the data with shortest path and consumes less energy. For that some network modules and energy usage modules in the proposed technique are to be created in which each node in the network broadcasts data so that each node is having its specific user id and connected to each other. Also, the node creates a topology without loss of data with shortest path and hence we get the required results at the destination end. In this paper implemented such a scheme and all results have been presented in the subsequent sections.

## Keywords

Vampire attacks, Stubborn, Disastrous, broadcasts

## 1. INTRODUCTION

Wireless technologies are being widely used today across the globe to support the communication needs of very large number of end users. Several data services include activities such as sending e-mail and instant messages, and accessing the web. The nodes transmit information through wireless medium. Mostly multiple nodes exist inside an area. There are typically large number of nodes in the battlefield environment that need to be interconnected including radios carried out by soldiers, radios mounted on vehicles, missiles unattended air vehicles (UAV), and sensors. In such an environment the network plays a critical role in the success of the military mission [1].

Wireless sensor network obtains information from distributed sensor node. These nodes can cooperate each other to improve the performance of the system. Usually, wireless sensor networks consist of hundreds or thousands of sensor nodes. Each node is capable of sensing, and transmitting the information.

The delivery of a packet to the destination is based on hop count routing, and needs total cooperation from the intermediate nodes. Sometimes a malicious node refuses to cooperate with host. It simply blocks, modifies or drops the traffic through it, by fooling the routing algorithm or even by choosing a strategic geographic path up to entire paths of the network. Wireless sensor networks are originally motivated by military application such as large scale and ocean surveillance [2].

For example, the design of MAC control protocols in the network. These protocols access the wireless channel, a misbehaving node and can easily change the MAC protocol behavior. MAC protocols play an important role in enabling normal network operation. Energy efficiency is the important thing in the MAC design as it refers to energy consumed for successful work. Since sensor nodes are usually battery operated ones, vampire attack is difficult to detect. It drains the battery power of nodes but easy to carry out by some technologies [1, 3].

## 2. RELATED WORK

This paper also covers some protocols like Ariadne, SAODV and SEAD, as these protocols share information with all nodes in the network. Denial of service attack in wireless network is centered on by overloading by target's resources. Because of denial of service attack, software is overloaded by attack and application fails. If sensor network encounters these types of attacks then it slowly reduces the functionality and performance of wireless adhoc sensor network. Denial of service attack is characterized by amplification, can amplify resources spends on attack [4, 5].

Attack on server resources is attempting to exhaust a server processing capabilities & potentially causing a denial of service attack. In distributed denial of service attack that began to attack public attention because of its distributed nature. It blocks the source node. A simple example is flooding attack that overwhelming its network. In this paper we proposed the method which will protect system from these types of attacks. Vampire attack effect on link state and distance vector protocol is used to find shortest path to all nodes in the network and link state. It sends nodes connectivity information to network [3-6]. Also, we made an effort to demonstrate how the vampire attack damages the system and how to recover using proposed scheme.

In initial work, demonstrated that how this attack works and gives permission to single packet to transverse in a series of loop. In another attack it constructs a long route, with independent hop count. Also suggested a technique over these attacks. Each node takes its independent decision. Whenever attack attempt signal goes, simultaneously topology is created. A node can be in sleeping or active state after sleeping for some time node can be active and goes into next state to handle the routing. A node is active when it knows some other node in the grid handle the routing [6, 7].

The delay is related to some neighboring node at that time the node becomes helper and count the remaining energy consumption. When the power is consumed it will split into parts like idle and sink or receive mode. When data is transmitted from source to sink, nodes relay the message. Each node that is being routed measures less hop count for shortest path and more hop count for longest path.

Whenever data is passed, the processor needs some nodes to create a topology and network. Sometimes it is possible that some nodes may lose the connectivity with other nodes. This happens just because of node goes to each other's transmission range. This result leads to collapse of established network & split into other parts.

Another possibility is that the node is completely disconnected from another node and disconnects the network because of battery power which will be either low or empty. So, at that time mobile adhoc network (MANET) will play an important role for transmission of data [8-10].

Vampire attacks are mainly divided into two type's i.e. stateless protocols and stateful protocol attacks. Along with this, it also defined for energy that to be consumed when protocols perform function. Stateless protocols are like the source routing protocols and source node specifies the route to sink within the packet header to carousel and stretch attack. Whenever process happens source node decides that the node is valid or not. If not, the valid node will be disabled. MAC layer require ground work which provide efficient support to network. When Mac layer becomes idle, potential packet connects to the same next hop & nodes are configured, Each node is neighbor of another node. [1, 11, 12].

Stateful protocols are the protocols in which nodes are aware of their topology. These are mainly divided into two states i.e. link state and distance vector. In these routing cases the cost to reach destination is calculated by means of hops between the source and the sink. Carousel attack composed looping route and stretch attack composed malicious route. Environmental disaster causes loss in the productivity and information.

The proposed system defines carousel and stretch attack, and protective security against these attacks. The proposed system main aim is to design secure transmission to achieve various adjectives in adhoc wireless networks and to ensure that the system is secure. There are different attack attempts like carousel & stretch to bypass the security control on to operating system. The success of an attack depends on vulnerability of particular operating system. These types of attack steal data from system sometimes modify the original data and to disrupt of operating system function as it takes malicious action. So, to protect the data, security feature implemented.

The main role of security mechanism is complete trust on node & hop count, because when packet is delivered to destination it measures the hop count. The current design of security transmission is better and protects the system. These processes use node ID, and verify & find particular address. If any malicious action occurred during transmission then it interrupts process & pointer immediately throw outside loop & this process continuous until honest path found. [13, 14]

## 3. PROPOSED SYSTEM

The proposed system design includes some modules. These modules work against vampire attack. In first attack whenever data is transmitted all nodes accept and send it to next state for further process. Looping route composed in a carousel attack and in case of second attack it creates long route as compared to carousel, we call it as malicious route composed in a stretch attack. Secure transmission is simple which finds the shortest path and sends the data to destination. The proposed system covers all the drawbacks of existing system and the data is transmitted at the destination end securely, and we found a honest path. Following are modules for this system -

- Network Creation Module
- Carousel Attack
- Stretch Attack
- Energy Level Identification
- Secure Transmission

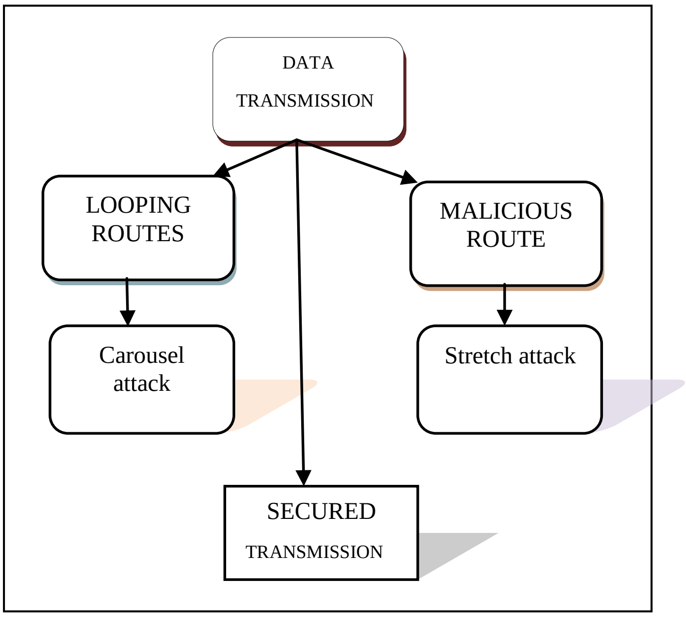

**Fig. 1: System architecture**

### 3.1 Network Creation Module

In the proposed module set up the network model with source, sink, and six intermediate nodes namely A, B, C, D, E, and F. Each of these nodes is having unique identity number. Because of the unique identity numbers, ambiguity does not arise during transmission of data. When any node fails or problem occurs, using ID no system can reach to that particular node. At every attempt of attack, node ID will be changed. And, the topology is created at the transmission time. In case of static protocols, topology is created during initial steup phase. Some times it will handle rare changes in the topology. Furthermore, node location in network is assumed to be fixed or random. Due to this network creation all the nodes are connected to each other. To configure the node here suggested new facility to user. Whenever entire node is configured, the neighboring node information can be obtained. During the transmission of data, each node knows its initial and next node, so that way of transmission of packets becomes easier [15].

### 3.2 Carousel Attack

In the carousel attack where source is at the initial stage and sink is at the last stage. Six intermediate nodes (A-F) are used for forming the loop. Using source, user selects the packet and sends packet with a route to sink. Intermediate node accepts the data and sends it to next node. The process creates a series of loop. Each node appears in the network many times in a circular order. Due to this, length of routes gets increased & seems it goes beyond the total number of nodes exists in the network. When data is transferred from source to destination (sink), topology is created & continuous loops will be created multiple times until source gets honest path. At the same time source node becomes a malicious one and loop will be created, with consuming energy and then process stops.

During this it takes time and battery power is also reduced significantly. It has target limited verification of data header from series of loop. Here routing loop creates and we call it as carousel attack.

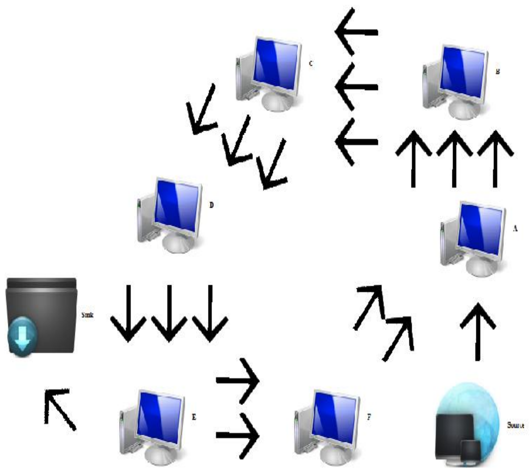

**Fig. 2: Carousel attack**

## 3.3 Stretch Attack

In this attack, the purpose is to source routing from initial to end phase. A rival constructs long routes as compared to carousel attack. The potential transmission includes from node A to node F in the network. Similarly, it also sends the data from source to destination. Node is completely independent of hop count. Whenever data is transmitted from source to sink malicious node creates a path. In case of stretch attack there may be possibility to loss the data. Honest node forms a shortest path but malicious node forms a longer path. Here topology is randomly generated. In case of carousel attack energy is consumed by factor of 4 while in stretch attack energy usage is by an order of magnitude, depends on location of malicious node. As it creates a long route, energy consumption is also increased. Whenever system sends the data as 10 or 100 packets, energy level consumed is different, as per the hop count. Each time it creates the longest route and energy consumed for each packet transmission. Here it forms the path as, source- A-B-C-D-E-Sink. This is the longest path as compared to carousel attack.

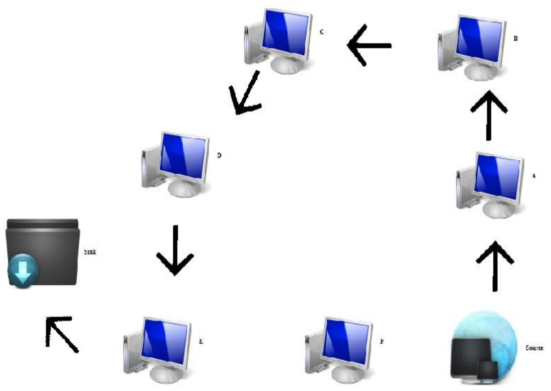

**Fig. 3: Stretch attack**

## 3.4 Energy Level Identification

The proposed module, shows energy level identification of each node. Before process starts, the energy level of each node is full. After every attack attempt happens the energy is reduced due to severe energy of sensor nodes network system design has a large impact on energy consumption and operational life time of whole network thus we did some process. When nodes battery power is reduced, it assumes that the energy is consumed. Nodes recharge their battery either continous charging or switching between active and recharge cycle. When nodes charge continously, power drain attack becames aggrasive. It consumes power before as far as node recharge. When battery power is full that means node is healthy. Before the start of process, node energy is full, as soon as nodes are configured , it enters in the process. Some times node will not take part in process or some times loss of data at that time node does not come in the path. Mostly, single attacker can use carousel attack so it affects power and more energy will be consumed [15, 16].

## 3.5 Secure Transmission

Security deals with confidentiality, integiry and the most importantly protection from end user or denial of service attack. Also, all of these things are coverd in the proposed technique. Here, the security is mainly used to prevent the system from vampire attack. So, secure transmission done in the node by overcoming the vampire attack. Secure transmission consists of energy level identification module with source, sink, and all six intermediate nodes. Each node is to be configured before actual process starts. Whenever data transmitted, it has to travel in the honest route, and it will mitigate the vampire attack. No backtracking property is satisfied for a given packet if and only if it consistently makes progress toward its sink level. There are equal no of hops in the network address space. In backtracking property, when every packet is transmitted from source to sink, it creates the number of hops. The intermediate nodes, which will work at source route. Now these intermediate nodes will work to find honest path. If node is disabled itself from the sink instead from the source, it will forward the loop that includes current node & sends data from source to destination with shotrest path. During the process energy is also consumed. Each node is having its specific identity number due to this each node gives its perticular address [15-18].

when process starts, nodes take their independent decision.and when receive the data, the sink gives the signal like “Message Received”. Then the user will know his data is reached to correct destination. All these processes are done securily. Therefore, source finds the honest path i.e. source-to sink using intermediate nodes (A-F). Following are the steps involved in implementing the proposed scheme.

**Step 1** Create six node A,B,C,D,E,F

**Step 2** Configure all the node A to F

**Step 3** Neighbouring node info found, check route

**Step 4** Send the data from source to destination

**Step 5** Data Transmitted from Node

**Step6** Using wireless sensor search valid path

**Step7** Ensure the path between node A to F

**Step 8** Final shortest path found

**Source –F-E-Sink**

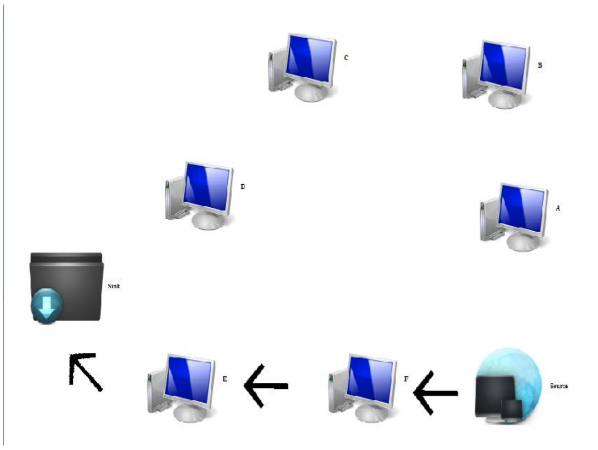

Fig. 4 : Secure transsmission

## 4. RESULTS & DISCUSSIONS

The model of the proposed scheme has been implemented in JAVA software. To understand the scheme introduced some attacks and observed their impact of these attacks on the system. Proposed technique evalutes shortest path using secure transmission in the wireless ad hoc sensor network. The result of attacks observered below with graphical representation. Energy has been consumed in each attack and route lengths are different for attacks. Nodes will transmit the data from source to sink, while transmission energy is consumed. All these results are analyzed in following graphical presetantion (Figures 5 to 8).

Energy usage & series of loop form is depicted in Carousel attack. One can observe , continuous looping may form & time consumed to find honest path upto sink. It refers entire network to transfer packets & all nodes receive message during transmission. Energy of all nodes in the network has been consumed.

Energy usage along with malicious route has been depicted in the stretch attack, looping is not continuous & may not refer all nodes in network to find honest path. Energy consumed only for nodes which received message & also less time consumed to find honest path than unlike Carousel attack. Also, with different packet loads i.e. Packet 1 to Packets 1000, the consumption of energy behaviour is different.

In this technique, source sends wireless signals to all network, it checks & determines honest path upto sink. The moment when source identifies short & nearest path without interruption to sink, it immediately sends packet to destination. Only nearest nodes to destination are included in secured transmission. The shortest path will be selected which requires less energy consumption (secured transmission). Overall, network is composed of different nodes & node energy distribution under different attacks are shown in Figures 5 to 8.

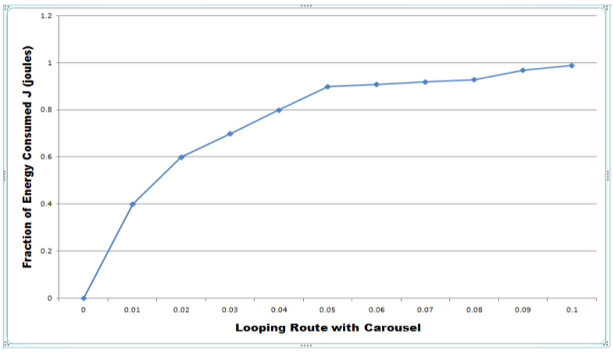

Fig. 5: Energy usages in carousel attack

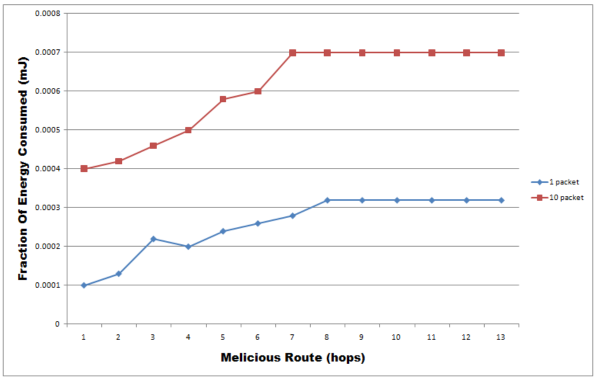

Fig. 6: Energy usages in stretch attacker with malicious route

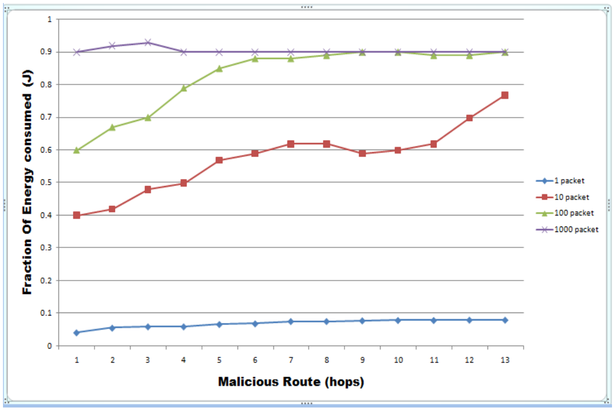

Fig. 7: Energy usages with stretch attacker with Number of packets

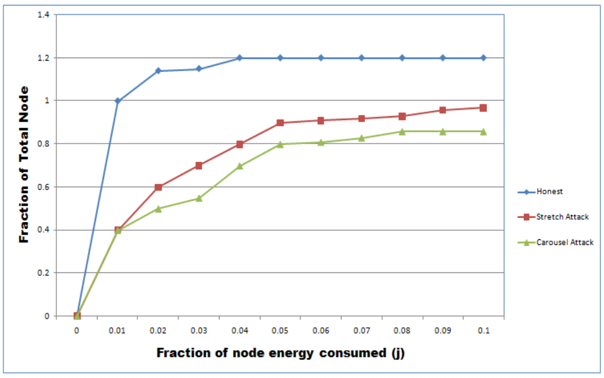

Fig. 8: Energy usages with secure transmission

## 5. CONCLUSION AND FUTURE SCOPE

Proposed technique creates all attacks and demonstrated how attacks attempt on system and how they damage to the system. Since proposed secure transmission is superior against the carousel and stretch attack, use of secure transmission saves times. The node id, network module, and energy level modules are adopted in the proposed technique. The proposed technique protects system against the vampire attack. During transmission of information nodes ensure that the battery power should be full. By proposed technique, it shows the shortest path creation and our data is transferred at the sink which consumes less battery power. Collection of damage bound, and handling mobile network is the future work.

## 6. REFERENCES

[1] Farooq Anjum and Petros Mouchtaris, *Security for Wireless Adhoc Network*, John Wiley & Sons Inc, 2007.

[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: a secure on demand routing protocol for ad hoc network," *MobiCom,* 2002.

[3] Manel Guerrero Zapata and N. Asokan,"Securing adhoc routing protocol," *WiSE*, 2002.

[4] Bryan Parno,Mark Luk,Evan Gaustad ,and Adrian perrig,"Secure sensor network routing: clean slate approach,"*CoNEXT*, 2006

[5] David B. Johnson, David A.Maltz, and Josh Broch DSR, "The dynamic source routing protocol for multihop wireless adhoc sensor network", *adhoc Networking,* 2001.

[6] Thomas H.Clausen and Philippe jacquet,"Optimized link state routing protocol*,"OLS),* 2003

[7] Haowen Chan and Adrian Perrig,"Security and privacy in sensor Network," *Computer*, vol. 36, no. 10. 2003.

[8] Gergely Acs, Levente Buttyan, Istvan Vajda,"Provably secure on demand source routing in mobile ad hoc network", *IEEE Transaction on Mobile Computing* vol. 05, no.11, 2006.

[9] John Bellard and Stefan Savage, "802.11denial of service attack: real vulnerabilities and practical solution," *USENIX security*, 2003.

[10] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, "*Strong* authentication for RFID system using the AES algorithm", *CHES*, 2004.

[11] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X.Brown, "An on demand minimum energy routing for wireless ad hoc network," *ACM SIDMOBILE Mobile Computing and Communication Review,* vol. 6, no. 3, 2006.

[12] Rahul C.Shah and Jan M. Rabaey, "Energy aware Routing for low energy ad hoc sensor network", *WCNC*, 2002.

[13] Vilkan Rodopu and Teresa H. Meng, "Minimum energy mobile wireless network*", IEEE Journal on Selected Area in Communication*, vol. 17, no.8, 1999.

[14] R.Govindan and A.Reddy, "An analysis of internet inter-domain topology and route stability," *INFOCOM,* 1997.

[15] Jiao Wen- Cheng, Peng Jing and Zheng Jain-Ling (2010), "Researches and improvement of AODVprotocol in ad hoc network*," Wireless Communication Networking and Mobile Computing (WiCom),* 2010.

[16] S. B. Lee and Y.H. Choi, "A secure alternate path routing in sensor network*"*, i*n Proc. of the Computer Communication*, vol. 30, pp.153-165, 2006.

[17] C. Karlof and D. Wagner*, "*Secure routing in wireless sensor network: Attack and Countermeasures*", University of California at Barkley. Tech. rep. F* 33615-01-c-1895.

[18] Frank Stajano and Ross Anderson, The resurrecting Duckling,*"* security issues for ad hoc wireless network*", International Workshop on Security Protocol,*1999.