ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

High Speed Data Communication with Improved Attack Detection Strategies in Wireless Sensor Networks

K.R.Raagavi[1], K.Ramachandran[2],

Department of Electronics and Communication Engineering, Mount Zion College of Engineering and Technology, Pudukkottai, India

Assistant Professor, Department of Electronics and Communication Engineering, Mount Zion College of Engineering and Technology, Pudukkottai, India

ABSTRACT: The main aim of this approach is to provide the trustworthy multi-hop routing between source and destination as well as establishing Sybil Attack detection support in wireless sensor network. Sybil Attack detection based wireless networks have evolved as a key and promising wireless technology for a large variety of applications ranging from home networking to transportation systems, defense and medical systems. Transmission Control Protocol (TCP) is a widely deployed transport protocol and its congestion control mechanisms guarantee reliable delivery of data and efficient allocation of network resources. Congestion control mechanisms implemented in TCP have evolved significantly to better the performance of TCP on different types of communication networks. Recently, a lot of research has focused on improving the performance of TCP connections with large congestion windows, resulting in new variants called “high-speed” TCP variants. In this system, we improve the performance of high-speed TCP variants in Sybil Attack detection wireless networks in terms of network throughput and expected throughput is used for comparison of throughput when nodes are mobile.

KEYWORDS: Sybil Attack, WSN, TCP, High Speed Data Communication.

I. INTRODUCTION

Wireless web technology has turned out to be well known lately because of the colossal development in the quantity of versatile registering gadgets and popularity for nonstop system network paying little respect to physical areas. Multi-hop remote systems, for example, Wireless Mesh Networks [WMNs], Mobile Ad-hoc Networks [MANETs], and so forth have risen as a promising remote innovation for a huge assortment of uses. Uses of multi-bounce remote systems go from broadband home systems administration, group systems administration and undertaking systems administration to restorative frameworks, security reconnaissance frameworks, transportation frameworks, guard and building mechanization. TCP has been broadly received as a solid information exchange convention for a large portion of the correspondence systems. In any case, viably and reasonably assigning assets of a system [e.g. transmission capacity] among a gathering of contending clients are real issues for a wide range of correspondence system.

A system is said to be congested when the activity offered to it surpasses the accessible limit. Van Jacobson laid the foundation for blockage control look into. He proposed another standard called "Preservation of Packets", which implies that another bundle is not infused into the system until an old parcel leaves the system. This rule prompts to the arrangement of a key component called "Self-Clocking", which implies that the source utilizes affirmations [ACKs] as a clock to decide when to send new parcels into the system. Van Jacobson proposed three calculations for clog shirking and control: Slow-Start, Congestion Avoidance and Fast Retransmit. Moderate Start calculation is intended to begin the Self-Clocking instrument. This calculation rapidly fills the unfilled pipeline [system is seen as a pipeline] toward the start of transmission or after a retransmission timeout to bring the association towards its harmony [an association is said to be in balance in the event that it is running steadily with a full window of information in travel].

Congestion/Traffic Avoidance calculation, otherwise called Additive Increase/Multiplicative Decrease calculation, nearly complies with the "Preservation of Packets" rule once the association is in balance. Quick Retransmit calculation considers copy affirmations as an indication of parcel misfortune in the system and retransmits the lost bundle without sitting tight for a retransmission clock to terminate. From that point forward, TCP clog control systems have experienced a few adjustments to enhance the execution of TCP on various sorts of correspondence systems. Late work in the range of blockage control concentrates on enhancing the execution of TCP associations with huge clog windows [cwnd]. The enhancements are centered around upgrading the fundamental instrument of AIMD to proficiently keep up the association at balance. In AIMD instrument, TCP sender upgrades the blockage window [cwnd] if an ACK is gotten or if the clog is recognized.

Floyd–Warshall Algorithm

In computer science, the Floyd–Warshall algorithm is an algorithm for finding shortest paths in a weighted graph with positive or negative edge weights (but with no negative cycles). A single execution of the algorithm will find the lengths (summed weights) of the shortest paths between all pairs of vertices.

Although it does not return details of the paths themselves, it is possible to reconstruct the paths with simple modifications to the algorithm. Versions of the algorithm can also be used for finding the transitive closure of a relation {\displaystyle R} R, or (in connection with the Schulze voting system) widest paths between all pairs of vertices in a weighted graph.

The Floyd–Warshall algorithm is an example of dynamic programming, and was published in its currently recognized form by Robert Floyd in 1962. However, it is essentially the same as algorithms previously published by Bernard Roy in 1959 and also by Stephen Warshall in 1962 for finding the transitive closure of a graph, and is closely related to Kleene's algorithm (published in 1956) for converting a deterministic finite automaton into a regular expression.

The modern formulation of the algorithm as three nested for-loops was first described by Peter Ingerman, also in 1962. The algorithm is also known as Floyd's algorithm, the Roy–Warshall algorithm, the Roy–Floyd algorithm, or the WFI algorithm.

Sybil Attack

The Sybil attack concerns the network layer of MANET. This kind of attack deletes all the data packets instead of sending them and consequently it makes the result of packet delivery ratio really low. The Sybil attack can be divided into two groups: single sybil attack and cooperative sybil attack; it depends on the aims of the attacker. In the first kind of sybil attack, the attack is applied via one of the existing nodes in the network, and in the other kind, the malicious nodes act in coordination with other attackers.

During the Route Discovery process, the source node broadcasts the RREQ message to its neighboring nodes to find a fresh path to the intended destination.

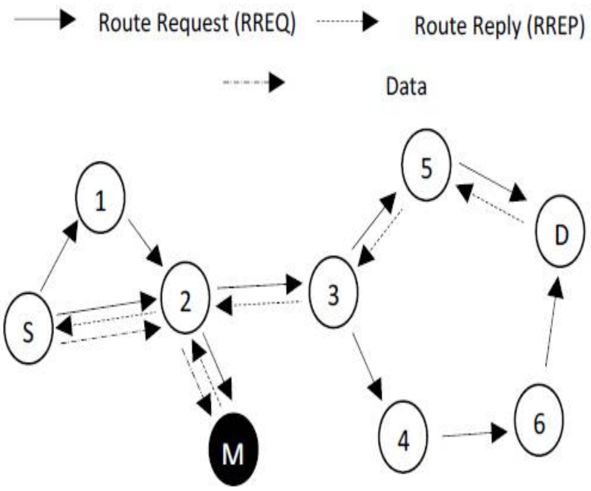


Fig.1. Attack Detection

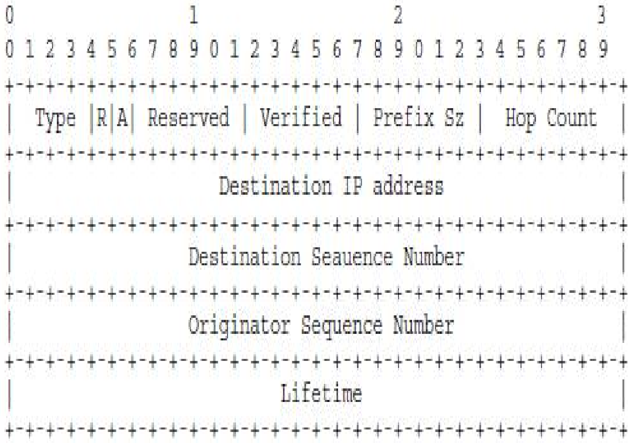
The sybil node immediately responds the source node with a RREP without checking its routing table for a fresh route to the destination packet. This packet reply includes the highest sequence number and is perceived as if it is coming from the destination node or from an intermediate node which has a fresh enough route to the destination node. The source node assumes that the process of the route discovery is done and discards the other RREP packets coming from other nodes, then selects the path through the malicious node to route the data packets. Therefore, the source node starts to send its data packets to the sybil node trusting that these packets will reach the destination node. The attacker now can drop the received data instead of relaying them as the protocol requires. The process of the sybil attack is schematized in the above figure.

Attack Prevention

In this prevention methodology, we will describe in details our proposed solution to prevent the sybil attack that we have integrated in the AODV routing protocol. Therefore, we slightly modify the recvReply(Packet *p), recvRequest (Packet *p) procedures and the Route Reply (RREP) message as shown in the following. Table 1 illustrates the fields of RREP message. According to the original AODV routing protocol, the source node has to broadcast the RREQ packet to find a path to reach the destination node. The destination node, or any intermediate node having the path, can send back the reply to the source node.

Then, by default, the source node accepts the first fresh enough RREP packet coming to it.

In our approach, like the standard AODV routing protocol, the destination node or intermediate node generates the RREP packet, but it also generates another RREP packet. It is a kind of confirmation of the first packet with a sequence number incremented by one.



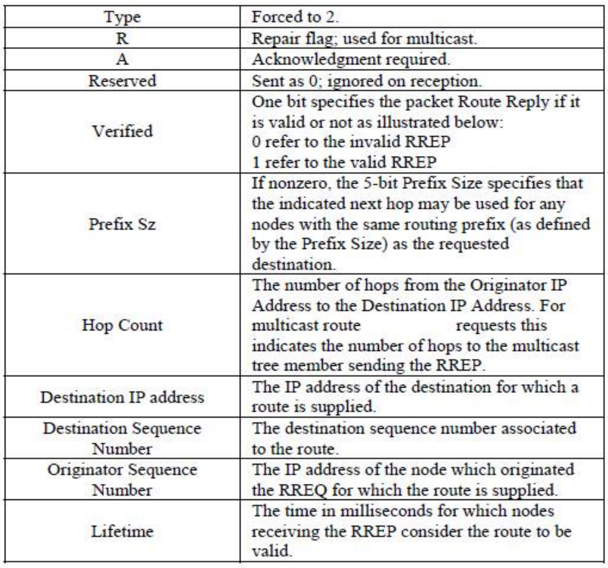
```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type |R|A| Reserved | Verified | Prefix Sz |  Hop Count  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Destination IP address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Destination Seauence Number                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Originator Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Lifetime                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 2. Format of the modified Route Reply (RREP) Message

Therefore, we have two RREP messages from the destination node or an intermediate node that has the route to the destination; one with the normal sequence number and the field VERIFIED set to 0. When the intermediate node receives the RREP packet it stores the information about the packet reply, then it checks our appended field VERIFIED if it is set to 0 or 1.

If it is 0, that means that our packet is not yet verified or it is an invalid packet. Otherwise the packet is verified and valid and it must be forwarded to the next node. In case of the field VERIFIED is 0 and the intermediate node receives a second route reply message, it must verify if the first route reply's sequence number is the second reply's sequence number minus one; if the verification is true, it sets the field VERIFIED to 1 and forward the packet. Also, when the intermediate node receives another route reply from the malicious node which performs sybil attack with a very high destination sequence number.

TABLE I. FIELDS OF RREP MESSAGE



Type	Forced to 2.
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Verified	One bit specifies the packet Route Reply if it is valid or not as illustrated below: 0 refer to the invalid RREP 1 refer to the valid RREP
Prefix Sz	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator Sequence Number	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

The same procedure explained will be repeated; and in this case the verification will be false, therefore, the intermediate node leaves the field VERIFIED set to 0 and ignores the packet.

Our solution avoids the sybil attack and also a multiple sybil attack. In addition, the control messages from the malicious node are not forwarded in the network. Our approach based on the four steps detailed below:

Algorithm Flow

```
Step 1: (Initialization Process)
Start the route discovery phase with the source node S.
Step 2: (Generation of RREPs)
The destination node or the intermediate node generates two route reply
with two different destination sequence number, the second one must be
incremented by one.
sendReply( seqno, // Dest Sequence Num
    VERIFIED = 0, ); // Appended field
sendReply( seqno+1, // Dest Sequence Num
    VERIFIED = 0, ); // Appended field
Step 3: (Verification of RREPs)
if ( intermediate node receives RREP ){
    if ( the first time the node receives RREP ){
        Store the IP address and seqno of the node;
        if ( RREP is valid){
            Forward RREP; }
    } else if (the node receives more than one RREP ){
        Store the IP address and seqno of the node;
        if ( RREP is invalid){
            if ( new RREP's seqno == old RREP's seqno + 1){
                VERIFIED = 1; //( Mark RREP as valid)
                Forward RREP;
            } else {
                Ignore RREP; }
        } else {
            Forward RREP; }
    }
}
Step 4: (Continue default process)
```

The source node sends data to the destination node from the selected route reply packet.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Coverage Area	500x500 m
Number of nodes	25
Simulation time	200s
Transmission range	50m
Mobility model	Random way point
Data Rate	0.25
Packet Size	512 Bytes
Routing Protocol	AODV / Modified-AODV
Mobility speed	0-30 m/s
No of black hole nodes	1 and 5
Connections	5
Traffic type	UDP–CBR
Pause time	10s

II. SYSTEM ARCHITECTURE

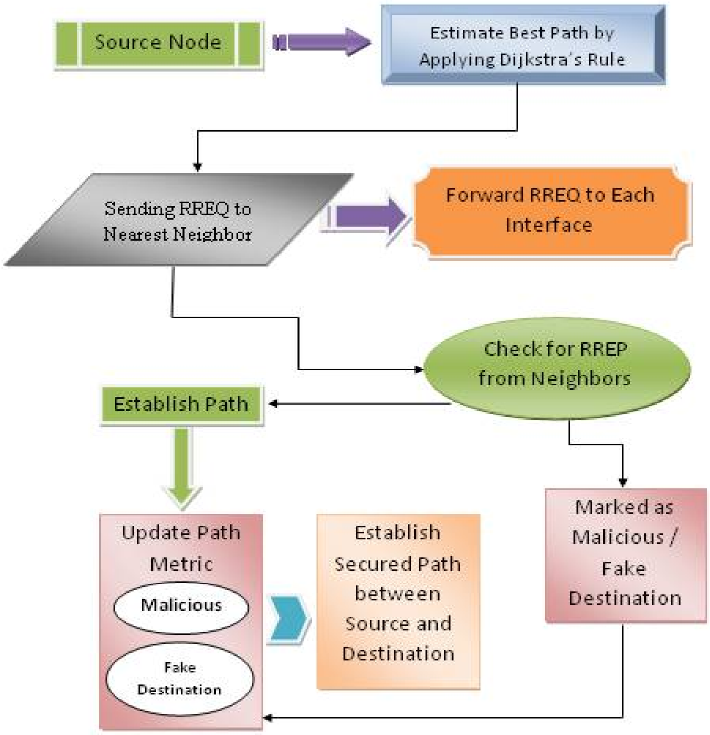

Source Node
Estimate Best Path by Applying Dijkstra's Rule
Sending RREQ to Nearest Neighbor
Forward RREQ to Each Interface
Check for RREP from Neighbors
Establish Path
Marked as Malicious / Fake Destination
Update Path Metric
Malicious
Fake Destination
Establish Secured Path between Source and Destination

Fig.3 System Architecture

DOI:10.15662/IJAREEIE.2017.0604079

III. LITERATURE SURVEY

A survey of attacks and countermeasures in mobile ad hoc networks - Wu, B., Chen, J., Wu, J., & Cardei, M. - 2007

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc network (MANET) will depend on people 's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. We provide a survey of attacks and countermeasures in MANET in this chapter. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks. First, we give an overview of attacks according to the protocol layers, and to security attributes and mechanisms. Then we present preventive approaches following the order of the layered protocol layers. We also put forward an overview of MANET intrusion detection systems (IDS), which are reactive approaches to thwart attacks and used as a second line of defense.

DoS attacks in mobile ad hoc networks: A survey - Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. - 2012

MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration, as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we will present survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Sybil attack and Gray hole attack which are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

A Taxonomy of Physical Layer Attacks in MANET - Khatri, S., Sharma, P., Chaudhary, P., & Bijalwan, A. - 2015

Mobile ad-hoc networks (MANETs) are a key enabler of pervasive computing. Constrained resources in mobile stations make it critical for nodes to be able to cooperate to enhance communication and computation capabilities. However, the wireless and dynamic nature of the links presents easy attack vectors for adversaries. The ability to securely discover and identify neighboring nodes (secure ND) is a fundamental building block for such networks. Even a relatively weak adversarial relay has the capability of distorting the network view and diverting significant amount of traffic. This can cause significant performance degradation. In this paper, we utilize the physical layer authentication scheme introduced by Yu, Baras and Sadler [1] to secure neighborhood discovery against adversarial relays. The proposed method incurs little performance overhead and requires no additional hardware. We provide analytical and simulation based performance evaluation of the security of our scheme.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

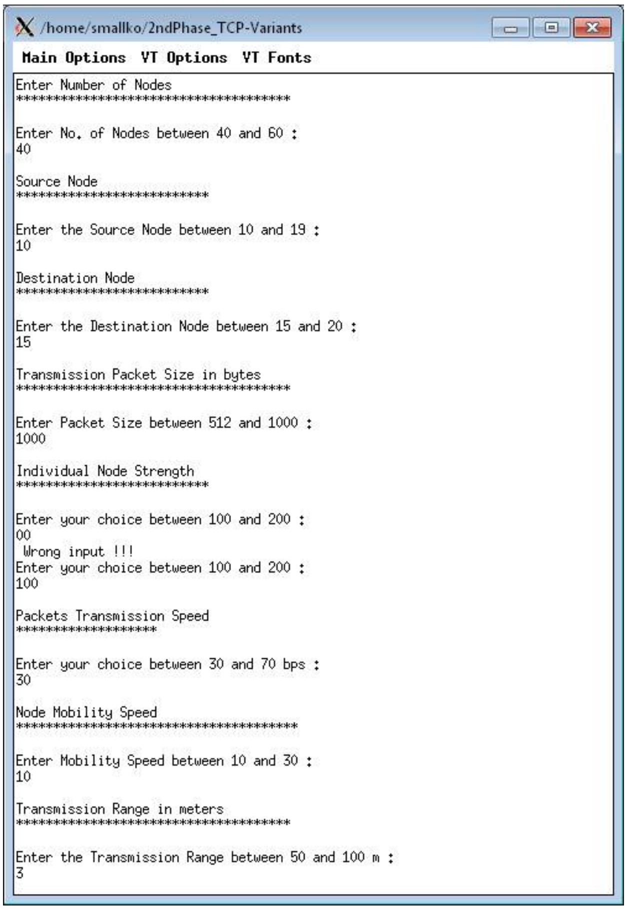
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

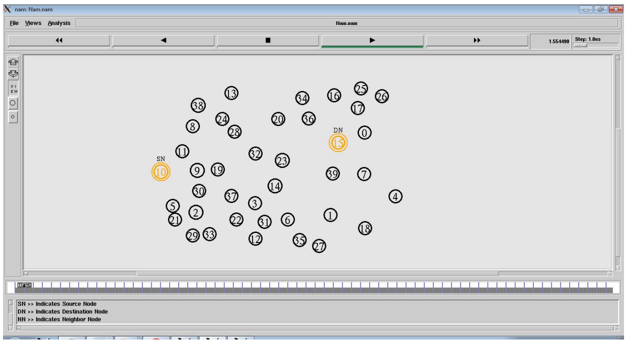
Vol. 6, Issue 4, April 2017

IV. EXPERIMENTAL RESULTS


/home/smallko/2ndPhase_TCP-Variants
Main Options VT Options VT Fonts

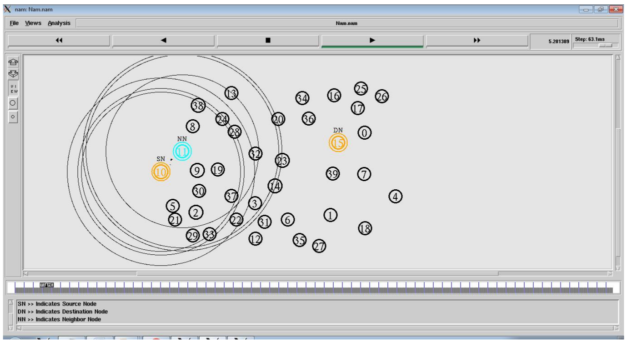
```
Enter Number of Nodes
*****************************************

Enter No. of Nodes between 40 and 60 :
40

Source Node
*****************************

Enter the Source Node between 10 and 19 :
10

Destination Node
*****************************

Enter the Destination Node between 15 and 20 :
15

Transmission Packet Size in bytes
*****************************************

Enter Packet Size between 512 and 1000 :
1000

Individual Node Strength
*****************************

Enter your choice between 100 and 200 :
00
 Wrong input !!!
Enter your choice between 100 and 200 :
100

Packets Transmission Speed
*********************

Enter your choice between 30 and 70 bps :
30

Node Mobility Speed
******************************************

Enter Mobility Speed between 10 and 30 :
10

Transmission Range in meters
*****************************************

Enter the Transmission Range between 50 and 100 m :
3
```

Fig. 4. Input Parameters



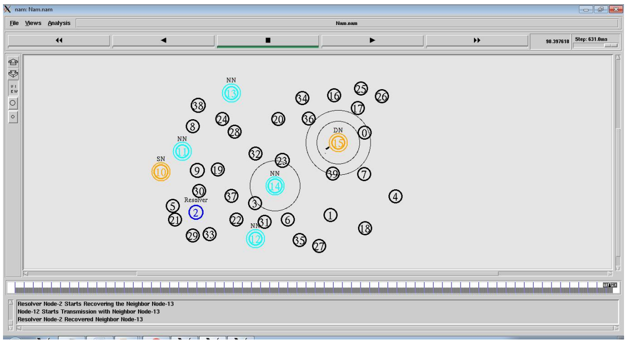
```
SN >> Indicates Source Node
DN >> Indicates Destination Node
NN >> Indicates Neighbor Node
```

Fig. 5. Node Formation



SN >> Indicates Source Node
DN >> Indicates Destination Node
NN >> Indicates Neighbor Node

Fig.6. Source and Destination Selection



Resolver Node-2 Starts Recovering the Neighbor Node-13
Node-12 Starts Transmission with Neighbor Node-13
Resolver Node-2 Recovered Neighbor Node-13

Fig.7. Communication.

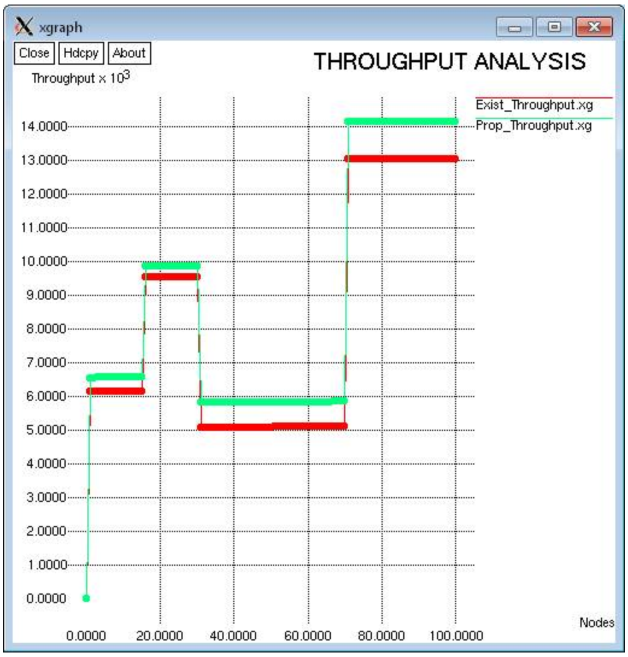


Fig. 8. Graphical Analysis of Throughput

DOI:10.15662/IJAREEIE.2017.0604079

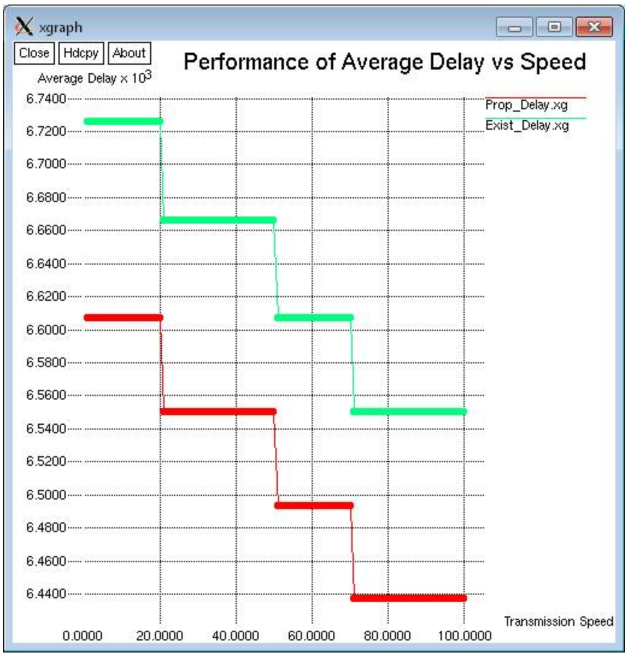


Fig.9. Graphical Analysis of Delay Vs Speed

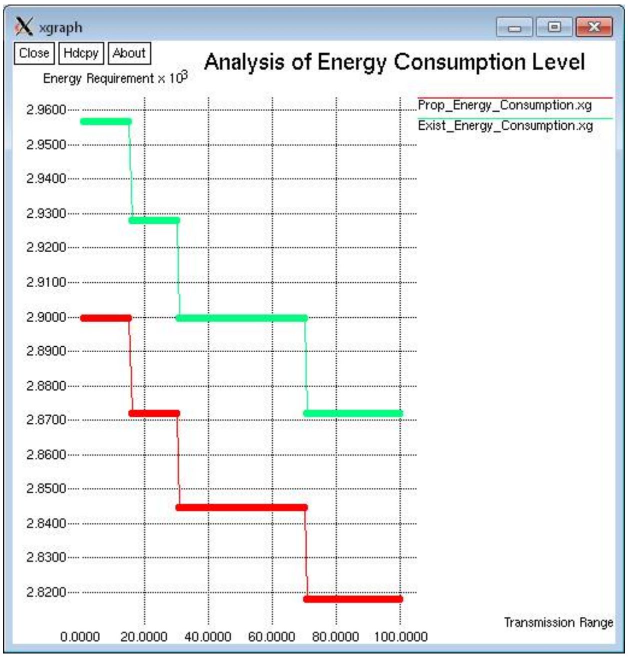


Fig.10. Graphical Analysis of Energy Consumption Level

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

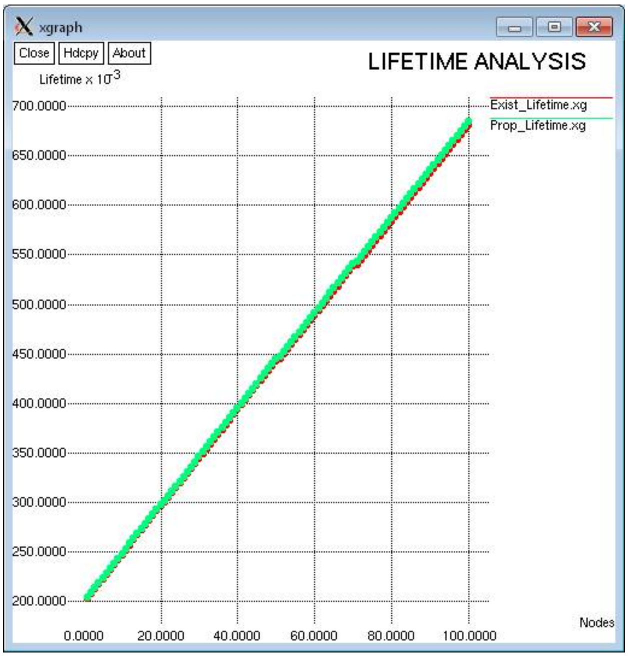


Fig11. Graphical Analysis of Network Lifetime

V. CONCLUSION

Through simulations we have studied the behavior of Sybil Attack detection and high-speed TCP variants in multi-hop wireless networks by varying the routing protocols such as Destination Sequenced Distance Vector (DSDV), Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) routing protocols. We have evaluated the performance of high-speed TCP variants in terms of throughput for static as well as mobile topologies. It is observed that the performance of TCP largely depends on routing protocols. Each routing protocol varies in the way it reacts to link failures. Routing protocols also differ in the way they form the routes. More routing overhead reduces the overall throughput of the network. More number of collisions due to increased routing overload makes the situation worse for TCP performance. Along with this we add the security parameters to identify the attacking nodes and using the resolver nodes to resolve the complete process and make the system more successful in all scenarios.

REFERENCES

[1] I. F. Akylidiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” Computer Networks, Elsevier, pp. 445-487, January 2005.

[2] T. Kelly, “Scalable TCP: Improving Performance in High Speed Wide Area Networks,” ACM SIGCOMM Computer Communication Review, vol. 33, pp. 83-91, 2003.

[3] V. Jacobson, “Congestion avoidance and control,” Proceedings of SIGCOMM ’88, ACM, Stanford, CA, Aug. 1988.

[4] K. Fall and S. Floyd, “Simulation-based comparisons of Tahoe, Reno, and SACK TCP,” ACM Computer Communication Review, vol. 26, no. 3, pp. 5-21, 1996.

[5] S. Floyd and T. Henderson, “The newreno modification to TCP’s fast recovery algorithm,” Request for Comments 2582, Experimental, April 1999.

[6] L. Brakmo and L. Peterson, “TCP Vegas: end-to-end congestion avoidance on a global internet,” IEEE Journal on Selected Areas in Communication, vol. 13, pp. 1465-1480, Oct. 1995.

[7] K. T. J. Song, Q. Zhang, and M. Sridharan, “A compound TCP approach for high-speed and long distance networks,” in Proceedings of PFLDNet, 2006.

[8] S. Floyd, “Highspeed TCP for Large Congestion Windows,” Request for Comments 3649, Experimental, 2003.

[9] L. Xu, K. Harfoush, and I. Rhee, “Binary Increase Congestion Control for fast long-distance networks,” in Proceedings of IEEE INFOCOM, Hong Kong, 2004.

[10] I. Rhee and L. Xu, “CUBIC: A new TCP-friendly high-speed TCP variant,” Proceedings of the third PFLDNet Workshop, France, 2005.
[11] C. Jin, D. X. Wei, and S. H. Low, “FAST TCP: motivation, architecture, algorithms, performance,” in Proceedings of IEEE INFOCOM, Hong Kong, 2004.
[12] TCP Evolution and Comparison, Which TCP will Scale to Meet the Demands of Today’s Internet? Whitepaper, FastSoft, Pasadena, 2008.
[13] G. Holland and N. Vaidya, “Analysis of TCP Performance over Mobile Ad Hoc Networks,” ACM/IEEE MOBICOM ’99, Seattle, Washington, Aug. 1999.
[14] E. D. Souza and D. Agarwal, “A HighSpeed TCP Study: Characteristics and Deployment Issues,” LBNL Technical Report, Berkeley, 2003.