ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Designing and Evaluating a Load Balanced IDS Environment in MANET Environment

E.Alwin Richared[1], R.Prasanth[2], K.Thulasiram[3], C.P.Gowthami[4]

U.G. Student, Department of ECE, GRT Institute of Engineering and Technology, Tamilnadu, India[1,2,3]

Assistant Professor, Department of ECE, G.R.T Institute of Engineering and Technology, Tamilnadu, India[4]

ABSTRACT: Developing and accessing secure MANET in real scenario is a tedious task that involves a secure design with reduced level of energy consumption. It is necessary one to operate over the continuous node processing system, as mobile nodes are resource constrained. In this project, we make a study about designing a secured cryptographic model. The intention of the study is to efficiently make use of all mobile nodes at the reduced level of energy consumption without compromising the security of nodes. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model. And the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system.

KEYWORDS: IDEA;IDS; MANET Security;hashing techniques

I. INTRODUCTION

MANET is actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks.Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)
- ProactiveMANET Protocol (PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed.

The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast
`forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues.
The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

II. RELATED WORK

1) Detecting and Overcoming Black hole Attack in Mobile Adhoc Network-2015
AUTHORS:Sakshi Jain, Dr. Ajay Khuteta
A mobile Adhoc Network (MANET) is a huddle of autonomous mobile nodes which dynamically forms a temporary multi-hoped radio network, without any use of previous infrastructure. Due to its characteristics like limited resources, changing topology and lack of centralized administration, MANET is exposed to various network layer attacks. Ad-hoc

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

On Demand Distance Vector (AODV) is a self-starting routing protocol for MANETs whose security is compromised with the particular type of attack called “BlackHole” attack.

2)Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks-2018
AUTHORS:TakuNoguchi ,Mayuko Hayakawa
A mobile ad hoc network (MANET) is a collection of mobile nodes that do not need to rely on a pre-existing network infrastructure or centralized administration. Securing MANETs is a serious concern as current research on MANETscontinuesto progress. Each node in a MANET acts as a router, forwarding data packets for other nodes and exchanging routing information between nodes. It is this intrinsic nature that introduces the serious security issues to routing protocols.

3)Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks - 2017
AUTHORS:TakuNoguchi ,Takaya Yamamoto
A mobile ad hoc network (MANET) is a collection of mobile nodes that do not need to rely on a pre-existing network infrastructure or centralized administration. Securing MANETs is a serious concern as current research on MANETs continuesto progress. Each node in a MANET acts as a router, forwarding data packets for other nodes and exchanging routing information between nodes. It is this intrinsic nature that introduces the serious security issues to routing protocols. A black hole attack is one of the well-known security threats for MANETs.

4)A Novel Taxonomy of Black-hole Attack Detection Techniques in Mobile Ad-Hoc Network (MANET) -2013
AUTHORS:AhmedSherif, MahaElsabrouty and Amin Shoukry
Mobile Ad-Hoc Networks (MANETs) are character- ized by the lack of infrastructure, dynamic topology, and their use of the open wireless medium. Black-hole attack represents a major threat for such type of networks. The purpose of this paper is two folds. First, to present an extensive survey of the known black-hole detection and prevention approaches. Another objective is to present new dimensions for their classification.Inparticular, the AODV protocol uses advertisements (HELLO messages) to discover their neighbors. When a source node wants to send a packet to a destination node it first broadcasts a Route Request message (RREQ) which is forwarded, through intermediate nodes, to their neighbors. When the (RREQ) reaches the destination node it responds by sending a unicast Route Reply message (RREP) to the source node.

5)A key management and secure routing integrated framework for Mobile Ad-hoc Networks -2013

AUTHORS:ShushanZhao , Robert Kent, AkshaiAggarwal

Key management (KM) and secure routing (SR) are two most important issues for Mobile Ad-hoc Networks (MANETs), but previous solutions tend to consider them separately. This leads to KM–SR interdependency cycle problem. In this paper, we propose a KM–SR integrated scheme that addresses KM–SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security features including confidentiality, integrity, authentication, freshness, and non-repudiation. Compared to symmetric cryptography, traditional asymmetric cryptography and previous IBC schemes, this scheme has improvements in many aspects. We provide theoretical proof of the security of the scheme and demonstrate the efficiency of the scheme with practical simulation. For key management, we can distribute security context in the form of symmetric keys or asymmetric keys. The latter includes certificate-based cryptography (CBC), and identity-based cryptography (IBC). Asymmetric key based schemes can provide more functionalities than symmetric ones, e.g., key distribution is much easier, authentication and non-repudiation are available, compromise of a private key of a user does not reveal messages encrypted for other users in the group.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

III. PROPOSED ALGORITHM

EXISTING SYSTEM

Existing security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols. SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network.

DISADVANTAGES OF EXISTING SYSTEM

- •More computation overhead.
- •Increase communication overhead.
- •Consumes more energy.
- •Detection of attackers not included.

PROPOSED SYSTEM

This paper proposes a novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control, and secure communication for MANETs using existing routing protocols. SUPERMAN combines routing and communication security at the network layer. This contrasts with existing approaches, which provide only routing or communication security, requiring multiple protocols to protect the network. SUPERMAN is a framework that operates at the network layer (layer 3) of the OSI model. It is designed to provide a fully secured communication framework for MANETs, without requiring modification of the routing protocol which process packets and provide confidentiality and integrity. SUPERMAN also provides node authentication. In this project, we make a study about designing a secured cryptographic model. The intention of the study is to efficiently make use of all mobile nodes at the reduced level of energy consumption without compromising the security of nodes. The study is focused into two steps. The first step concentrates on developing an enhanced IDEA cryptography model. And the second step focuses on balancing the loads of IDS nodes in order to reduced energy usage. Our novel proposed systems works independently towards each other under secured environment. Experimental analysis will prove the effectiveness of the system.

ADVANTAGES OF PROPOSED SYSTEM

- •Increase accuracy rate on detection DDos attack
- •Decrease communication overhead
- •Increase network lifetime.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

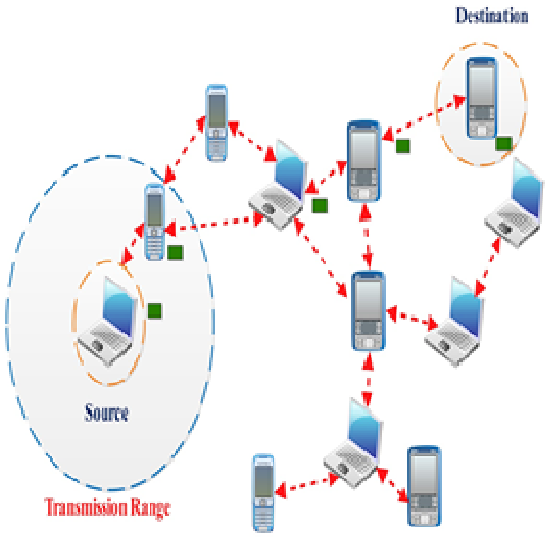
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

SYSTEM ARCHITECTURE



MODULES DESCSRIPTION

Network Topology

The sensor nodes are randomly distributed in a sensing field. We are using mobile ad hoc network (MANET). This is the infra structure less network and a node can move independently. In a MANET, each node not only works as a host and also acts as a router. We can find the communication range for all nodes. Every node communicates only within the range. If suppose any node out of the range, node will not communicate those nodes or drop the packets.

The Superman Framework

SUPERMAN is a framework that operates at the network layer (layer 3) of the OSI model. It is designed to provide a fully secured communication framework for MANETs, without requiring modification of the routing protocol. It shows the flow of data from transport, through the network layer (including SUPERMAN) to the data link layer. The dashed boxes represent elements of SUPER-MAN that process packets and provide confidentiality and integrity. SUPERMAN also provides node authentication.

Key Management

SUPERMAN relies on the dynamic generation of keys to provide secure communication. The Diffie-Hellman key-exchange algorithm provides a means of generating symmetric keys dynamically and is used to generate the SK keys. SKbkeys can simply be generated by means of random number generation or an equivalent secure key generation service.

Secure Node-to-Node Keys

SKekeys are used to secure end-to-end communication with other nodes, with one SKekey generated per node, for every other node also authenticated with the network. SKpkeys are used for point-to-point security and generated inthe same manner as SKekeys. It is important that SKeandSKpkeys are different, as the network needs to secure both the content of a packet and the route taken. A KDF can be used to generate these two keys in con-junction with the result of the Diffie-Hellman algorithm, requiring a DKSp/DKSprivpair, to minimise the cost of security on the network and reduce the key re-use and, in turn the lifetime of each key.These keys are generated when nodes receive DKSp's from other SUPERMAN nodes.

Secure Point-to-Point Footers

Secure footers are appended to all communication packets sent between SUPERMAN nodes. SKbpandSKp(x)keys are used in broadcast and unicast integrity service provision respectively. An example tag generation algorithm is the Hashed-Message Authentication Code (HMAC) which provides integrity and authenticity

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

services to a packet. A digest of the packet is generated, encrypted with the appropriate key (SKbp or SKp(x)), and appended to the packet. This tag is removed, checked and regenerated at each hop

Secure Broadcast Keys

At initialization of the network, the first node to be contacted about joining the network will generate a symmetric network key (SKb). This key is sent to all nodes that authenticate with the network. This key provides the basis for all broadcast communication security in a SUPERMAN network. The SKbis processed by the function KDF (SKb, type) into two broadcast keys (SKbe and SKbp). A node will use these keys to encrypt and sign packets sent to the broadcast address of the network. This key is used for broadcast and multicast communication, such as MANET route updates. It is not used for communication between individual end-points.

Performance Evaluation

In this section, we can evaluate the performance of simulation. We are using the xgraph for evaluate the performance. We evaluate our proposed method with respect to the following metrics: Packet Delivery Ratio, Energy Consumption and End to end delay. These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output.

IV. SIMULATION RESULTS

Simulation has been done using network simulator (NS2.28 in the area of 1500m * 1500m. Simulation setup is described in this section. The development of NS-2 is an oriented object program where two languages are used: C + + and Tcl. NS-2 supports a variety of protocols, providing simulation results for both wired and wireless It can also be used as a network simulator with limited functionality. It is popular in academia for its scalability (due to its open source model) and the online documentation abundant.

Below represents additional parameters used during simulation.

```
setval(chan)            Channel/WirelessChannel ;# channel type
setval(prop)            Propagation/TwoRayGround        ;# radio-propagation model
setval(netif)           Phy/WirelessPhy         ;# network interface type
setval(mac)             Mac/802_11                      ;# MAC type
setval(ifq)             Queue/DropTail/PriQueue ;# interface queue type
setval(ll)                      LL                      ;# link layer type
setval(ant)             Antenna/OmniAntenna     ;# antenna model
setval(ifqlen)          50                              ;# max packet in ifq
setval(nn)              59                              ;# number of mobilenodes
setval(rp)              SAODV                           ;# routing protocol
setval(energymodel)             EnergyModel
setval(x)                       900             ;# X dimension of topography
setval(y)                       900             ;# Y dimension of topography
```

Once the code « main.tcl » is debugged, the window below appears to start the simulation.

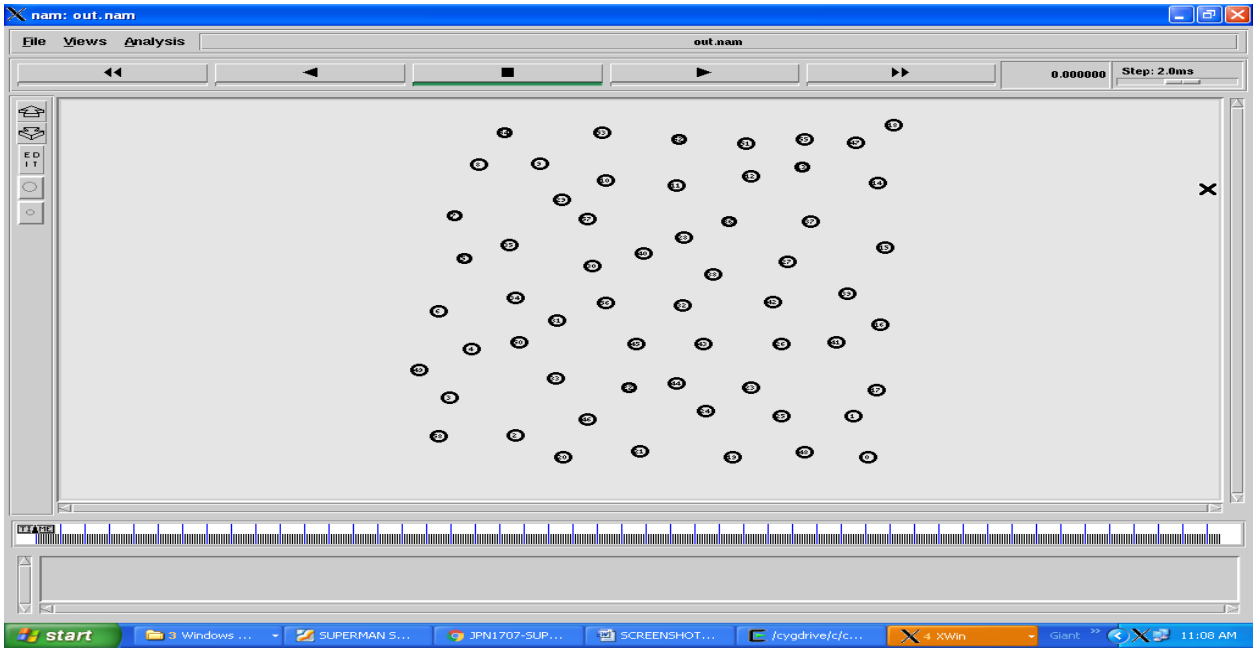
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

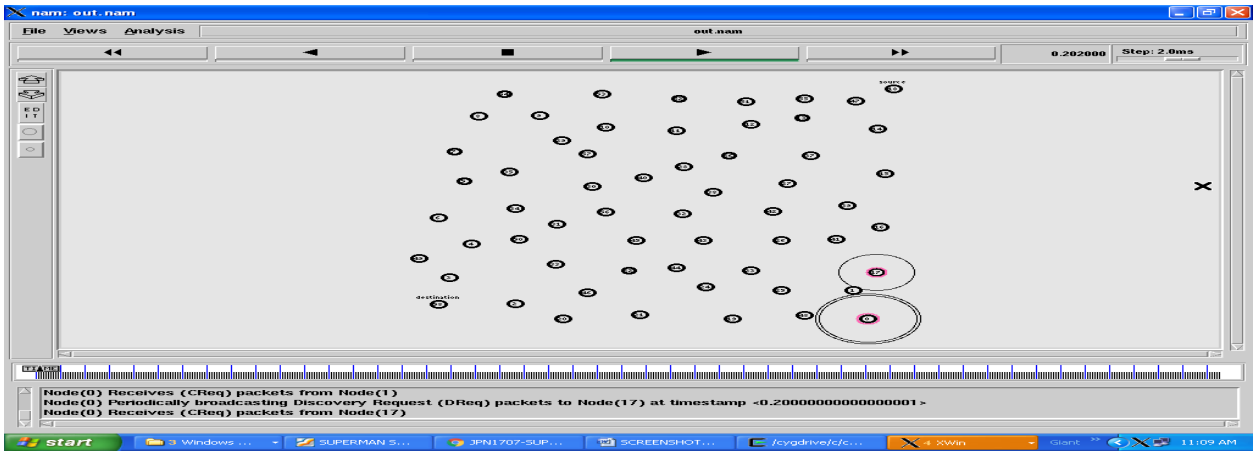
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019



The above figure shows the nodes creation the maximum number of nodes used here is 59. Let's assume a network in which MANET has formed a topology shown in above. Node S and D are source and destination respectively, N1, N2... N8 represents the intermediate nodes. Route discovery is started by source node S.



In the above the node "1" checks the route data between Nearest Neighbor node by sending RREQ and RREP.It will repeats until it reached Node "59". Based on generated route reply, destination node decides the priority for each path. While assigning priority, destination checks whether two path has same route cost and assigns based on delay if found. That means a route which has less delay value will get higher priority than other. Route discovery is started by node S by broadcasting the route request (RREQ) in the network. Route request packet initializes timestamp, total residual energy, minimum residual energy and delay values. All neighbor of S, N1, N3, N5 will receive the RREQ and extract.

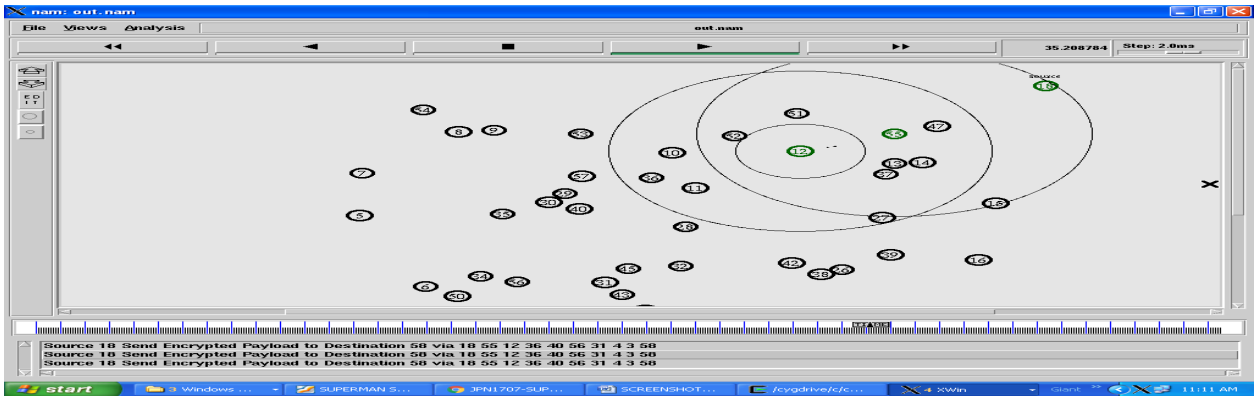
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

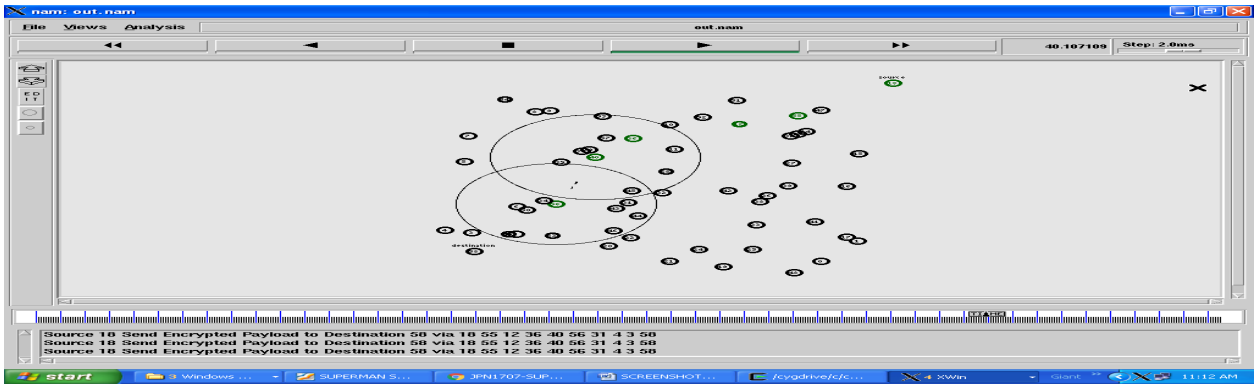
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

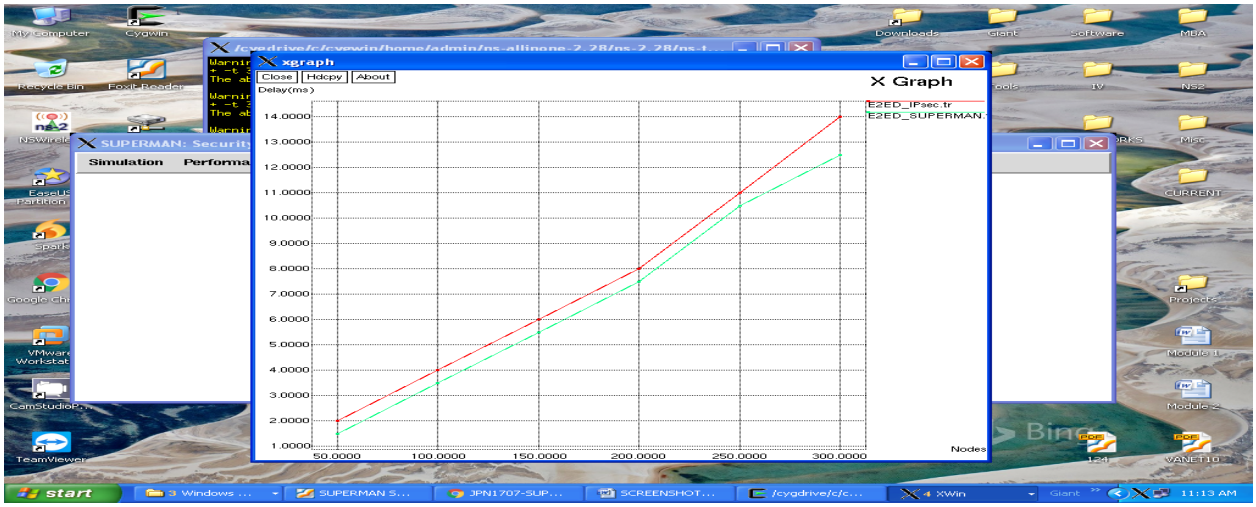
Vol. 7, Issue 2, February 2019



In the above figure shows the node 10 sends the Encrypted payload to destination 50 via 10 55 12 36 40 56 31 4 3 58



In the above figure shows the green color nodes are the final encrypted path for the data sends from node 10 sends the Encrypted payload to destination 50 via 10 55 12 36 40 56 31 4 3 58



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Performance Evaluation

In the above figure shows End-to-End delay is the average time taken for a packet to be transmitted from the source to destination. The lower value of end to end delay means the better performance of network.

The above figure shows end to end delay of proposed protocol compared to existing approaches. It shows end to end delay of Existing Method is very high compared to Proposed Method. This is because it mainly focuses on the maximum number of packet delivery irrespective of the delay hence increased

Figure 6.7 Packet Delivery Ratio

Packet delivery ratio is the ratio of the number of packet received at destination and number of packet sent by the source. The greater value of packet delivery ratio means the better performance of network.

The above figure shows that the ratio of packets loss occurred due to the attackers node or link error appears in the packet transmission between the nodes

V. CONCLUSION AND FUTURE WORK

SUPERMAN has been shown to provide lower-cost securitythan SAODV and SOLSR for their respective routingprotocols. By establishing a secure, closed network; onecan assume a certain level of trust within that network.This reduces the need for costly secure routing behaviorsdesigned to mitigate the effects of an untrusted environment (and untrusted nodes) on the routing process. By preventingthe entry of potentially untrustworthy nodes to thenetwork, and thus the routing process, a MANET may beprotected from subversion of its routing services at a lowercost, as malicious nodes are barred from the process entirely.SUPERMAN provides security to all data communicatedover a MANET. It specifically targets the attributesof MANETs; it is not suitable for use in other types of networkat this time. It sacrifices adaptability to a range of networks,to ensure that MANET communication is protectedcompletely and efficiently. A single efficient method protectsrouting and application data, ensuring that the MANETprovides reliable, confidential and trustworthy communicationto all legitimate nodes.

REFERENCES

1. P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.
2. Chandra, “Ontology for manet security threats,” PROC. NCON, Krishnankoil, Tamil Nadu, pp. 171–17, 2005.
3. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
4. D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, “A cluster-based approach to consensus based distributed task allocation,” in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.
5. D. Chakeres and E. M. Belding-Royer, “Aodv routing protocol implementation design,” in Distributed Computing Systems Workshops, 2004. Proceedings.24th International Conference on. IEEE, 2004, pp. 698–703.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

6. T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennotet al., "Optimized link state routing protocol (olsr)," 2003.
7. M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.
8. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.
9. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38– 47, 2004.
10. N. Garg and R. Mahapatra, "Manet security issues," IJCSNS, vol. 9, no. 8, p. 241, 2009.
11. Ivancic, D. Stewart, D. Sullivan, and P. Finch, "An evaluation of protocols for uav science applications," 2011.
12. R. McGee, U. Chandrashekhar, and S. H. Richman, "Using itu-t x. 805 for comprehensive network security assessment and planning," in Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International. IEEE, 2004, pp. 273–278.
13. M. G. Zapata, "Secure ad hoc on-demand distance vector routing," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106–107, 2002.
14. F. Hong, L. Hong, and C. Fu, "Secure olsr," in Advanced Information Networking and Applications, 2005. AINA 2005.19th International Conference on, vol. 1. IEEE, 2005, pp. 713–718.
15. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure, "Secure extension to the olsr protocol," in Proceedings of the OLSR Interop and Workshop, San Diego, 2004.
16. R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.
17. S. Maity and S. K. Ghosh, "Enforcement of access control policy for mobile ad hoc networks," in Proceedings of the Fifth International Conference on Security of Information and Networks. ACM, 2012, pp. 47–52.
18. D. Hurley-Smith, J. Wetherall, and A. Adekunle, "Virtual closed networks: A secure approach to autonomous mobile ad hoc networks," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015, pp. 391–398.
19. S. Bhattacharya and T. Basar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in American Control Conference (ACC), 2010. IEEE, 2010, pp. 818–823.
20. S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," in Computational Intelligence and Security, 2009. CIS'09.International Conference on, vol. 2. IEEE, 2009, pp. 421–425.
21. S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.
22. M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," RFC 2560, Tech. Rep., 1999.
23. N. Doraswamy and D. Harkins, IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.
24. Ghosh, R. Talpade, M. Elaoud, and M. Bereschinsky, "Securing ad-hoc networks usingipsec," in Military Communications Conference, 2005. MILCOM 2005.IEEE. IEEE, 2005, pp. 2948–2953.
25. N. Ali, M. Basheeruddin, S. K. Moinuddin, and R. Lakkars, "Manipsec-ipsec in mobile ad-hoc networks," in Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 1. IEEE, 2010, pp. 635–639.
26. Harn, M. Mehta, and W.-J.Hsin, "Integrating diffie-hellman key exchange into the digital signature algorithm (dsa)," Communications Letters, IEEE, vol. 8, no. 3, pp. 198–200, 2004.