IJSEAT International Journal of Science Engineering and Advance Technology

Efficient and Secure Routing In Network Layer For MANET

[1]L.Samuel James, [2]P.Radhika Krupalini

[1]Final Master of Science in Computer Science, Ideal college of Arts and Sciences.,Vidyuth Nagar,Kakinada,E.G.Dist.,A.P.,India.

[2]Associate professor, Dept of Computer science,Ideal college of Arts and Sciences., Vidyuth Nagar,Kakinada,E.G.Dist.,A.P.,India.

ABSTRACT:
Secure routing and communication security protocols can be combined and applied on the messages to deliver them with complete shielding. The custom of communication security protocols initially advanced for wire line and Wi-Fi networks can also present a heavy burden on the limited network resources of a MANET. To discourse these issues, a novel secure framework (SUPERMAN) was projected. The basis is planned to consent existing network and routing protocols to complete their functions, while providing node authentication, access control, and communication security mechanisms. In this work we present innovative security framework for MANETs, SUPERMAN. Recreation results comparing SUPERMAN with IPsec, SAODV and SOLSR are provided to determine the suggested frameworks correctness for wireless communication security.

KEYWORDS: control traffic, topology, broadcast, manets, security protocols

1 INTRODUCTION

MANETs are lively, self-configuring, and infrastructure-less groups of mobile devices. They are typically meant for a precise determination. Each maneuver within a MANET is identified as a node and must take the role of a client and a router. Communication across the system is accomplished by forwarding packets to a destination node; when a direct source-destination link is unreachable intermediate nodes are used as routers. Mobile ad hoc network (MANET)statement is regularly wireless. Wireless communication can be irrelevantly captured by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route guidance attacks that can conciliate the integrity of the network. Mobile networked systems have seen improved usage by the military and commercial sectors for tasks estimated too monotonous or hazardous for humans.

2 LITERATURE SURVEY

2.1 We define the event triggers required for Ad hoc On-demand Distance Vector (AODV) operation, the enterprise promises and the decisions for our (AODV) routing protocol employment. This paper is intended to aid researchers in developing their own on-demand ad hoc routing protocols and promoting users in influencing the employment design that best fits their needs.

2.2 By dwindling communication range and instigating multi-hop routing between nodes, while warranting network connectivity is upheld, spatial multiplexing of the wireless channel is exploited. The proposed procedure is assessed using the OPNET network simulation tool for the Greedy Perimeter Stateless Routing (GPSR), Optimized Link State Routing (OLSR), and Ad hoc On- demand Distance Vector (AODV) routing protocols in the setting of a swarm of UAVs.

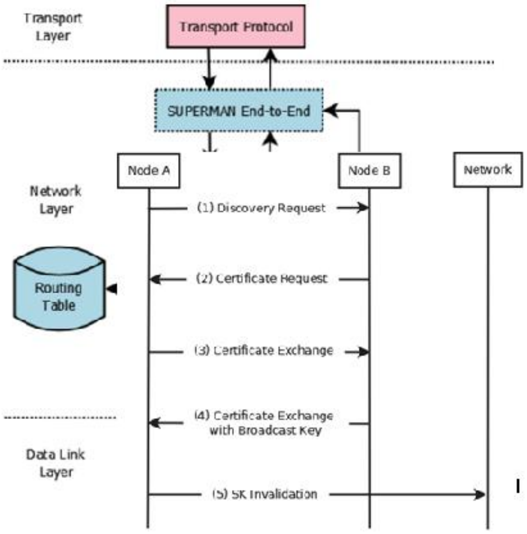
3 PROBLEM DEFINTION

Reactive protocols such as Ad hoc On-demand Distance Vector (AODV), propose routes when messages need to be sent by voting nearby nodes to discover the shortest route to the destination node. Alternative system - Optimized Link State Routing (OLSR) takes an upbeat style, intermittently submerging the network to engender routing table entries that keep it up until the next update. Both approaches are motion-tolerant and have been instigated in Unmanned Aerial vehicle(UAV)MANETS.

4PROPOSED APPROACH

SUPERMAN associates routing and communication security at the network layer. This diverges with current approaches, which deliver only routing or communication security andmanifolds protocols to protect the network.SUPERMAN is anoutline that operates at the network layer (layer 3) of the OSI model. It is intended to deliver a completely secured communication framework for MANETs, withneedful modification of the routing protocol which process packets and provideprivacy and integrity. SUPERMAN also provides node verification.

5SYSTEMARCHITECTURE



6 PROPOSED METHODOLOGY

6.1 System Construction

We customize multi-nodes as the router node and client-server node. Entirely we are taking multi-nodes in our system. Bothhostsareassociated via routers. Each host has manifold paths to reach a single terminus node in the network. The nodes are related by duplex link connection. The bandwidth for each link is 100 mbps and delay time for each link is 10 ms. Each edge uses Drop Tail Queue as the boundaryamongst the nodes.

6.2 Key Management

Packet type indicates the purpose of the packet. Timestamps provide unique identitylettingthe discovery of packets which are replayed thus ensuringfoundation for non-repudiation of packets sent earlier. SUPERMAN trusts on the lively generation of keys to deliver secure communication. The Diffie-Hellman key-exchange procedureoffers a means of making symmetric key generation possible and is acastoff to make the Symmetric Keys (SK) keys. Symmetric Broadcast keys (*SKb)* can only be produced by means of an algorithm that generates random numbers or acorrespondingprotected key generation service.

6.3 Secure Node-to-Node Keys

Security keys for encryption (*SKe* keys) are used to secure end-to-end communication with other nodes, with one *SKe* key made per node, for each node genuine with the network. Security keys per pair of nodes (*SKp* keys) are used for point-to-point security and made in the same manner as *SKe* keys. It is important that *SKe* and *SKp* keys are dissimilar, as the network needs to safeguard both the packet data and the route traversed.

6.4 Storage

SUPERMAN stores keys in each node's encrypted table. The security table comprehends the security permits of nodes with which the node has communicated earlier. This table has *n* entries, where *n* is the number of nodes that the node in enquiry has earstwhile communicated with Table has switchedIDs with two other nodes, X and Y.

6.5 Communication Security

Discretion and varietycombined and implemented in cryptographic algorithm will give rise to an encrypted payload(EP).when secure data is circulated over multiple hops, it

Should be trustworthy.This is accomplished using a hashing algorithm such as HMAC.Thus the packet's journeyfrom point-to-point until thedestination is reached is pragmatic.

7SECURITY FRAMEWORK:

INPUT: NODES, TA, PUBKEY, PRIKEY

STEP1: Node is provided with a certificate from a TA

STEP2: The joining nodeA seeks to join a network by periodically broadcasting Discovery Request packets containing its Public Diffie-Hellmen Key Share(*DKSp)*. This continues until it receives a Certificate Request from a networkable nodeB.

STEP3: *A* sends its certificate in a Certificate Exchange packet to *B.*

STEP4:B checks the integrity and authenticity of the Certificate Exchange(CEx)packet, using the shared SKp.

STEP5: If the certificate is deemed authentic A is added to B's security table.

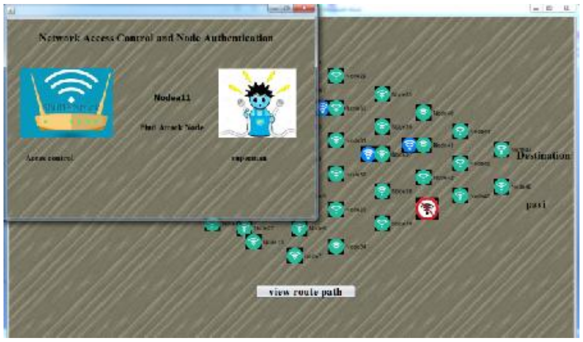
If the certificate fails this check, the DKSp, SKe and SKp credentials generated for node A by B aredropped and B and the process ends.

STEP6: If B has not yet authenticated any other nodes, it will generate an *SKb*, prior to sending it to the joining node,otherwise it will send the current *SKb* to the joining node.

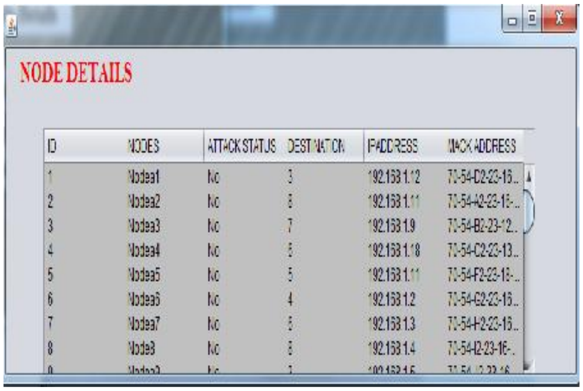
STEP7: If *A* has a broadcast key, it transmits a Broadcast Key Exchange (*BEx*) packet containing the new key, secured with the original key before committing the new key to its security table.

STEP8: *B* broadcasts an SK Invalidation (*SKI)* packet, invalidating any previous credentials *A* may have had with nodes within the network. This prevents the accumulation of expired security data on nodes that may be isolated from a previous invalidation event.

8RESULTS:

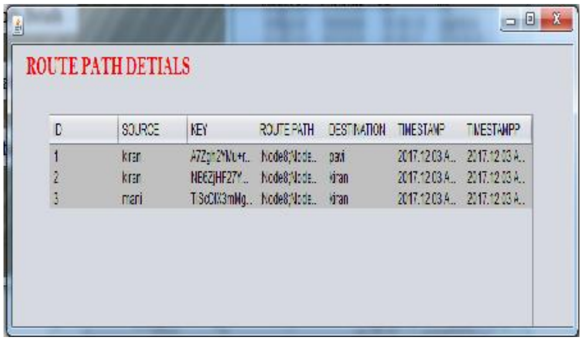


Access control and Node Authentication Network


NODE DETAILS

ID	NODES	ATTACK STATUS	DESTINATION	IPADDRESS	MACK ADDRESS
1	Nodea1	No	3	192.168.1.12	70-54-D2-23-16...
2	Nodea2	No	8	192.168.1.11	70-54-A2-23-16-...
3	Nodea3	No	7	192.168.1.9	70-54-B2-23-12...
4	Nodea4	No	5	192.168.1.18	70-54-C2-23-13...
5	Nodea5	No	5	192.168.1.11	70-54-F2-23-16-...
6	Nodea6	No	4	192.168.1.2	70-54-G2-23-16...
7	Nodea7	No	5	192.168.1.3	70-54-H2-23-16...
8	Node8	No	8	192.168.1.4	70-54-I2-23-16-..
9	Nodea9	No	7	192.168.1.6	70-54-J2-23-16

Node Details


ROUTE PATH DETIALS

ID	SOURCE	KEY	ROUTE PATH	DESTINATION	TIMESTAMP	TIMESTAMPP
1	kiran	A7Zgn2*Nu+r..	Node8;Node..	pavi	2017.12.03 A...	2017.12.03 A...
2	kiran	NE6ZjHF27Y...	Node8;Node..	kiran	2017.12.03 A...	2017.12.03 A...
3	mari	TSdCIX3mMg..	Node8;Node..	kiran	2017.12.03 A...	2017.12.03 A...

Route Path Details

EXTENSION WORK:

Design a routing policy with improved delay performance and the design of Distributed Opportunistic Routing with Congestion Diversity proposing a time-varying distance vector, which enables the network to route packets through a neighbor with the least estimated delivery time.

9CONCLUSION

SUPERMAN has been revealed to offer lower-cost refuge than SAODV and SOLSR for their individual routing protocols. By creating a secure, closed network; one can accept a positive level of trust inside that network. This diminishes the need for inflated secure routing deedsconsidered to allay the things of an untrusted environment on the steeringcourse. By foiling the access of hypotheticallydisloyal nodes to the network, and the overwhelming process, a MANET may be dwindling from mutiny of its routing facilities at a lower cost, as malicious nodes are barred from the process entirely. A single proficienttechnique protects steering and application data, safeguarding the MANET that deliversdependable, intimate and trustable communication to all genuine nodes.

10REFERENCES

[1]P.S. Kiran, "Protocol architecture for mobile ad hoc networks," *2009 IEEE International Advance Computing Conference (IACC 2009)*, 2009.

[2] A. Chandra, "Ontology for manet security threats," *PROC. NCON*, *Krishnankoil*, *Tamil Nadu*, pp. 171–17, 2005.

[3]A. 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] I. 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.

[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot *et 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]J. 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]W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, “An evaluation of protocols for uav science applications,” 2011.

[12] A. 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]A. 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]Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle, SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks,2017

L.Samuel James is student of Computer Science Department at IDEAL COLLEGE OF ARTS AND SCIENCES,KAKINADA, AP, INDIA.Presently he is pursuing his final semester in Master of Science in Computer Science from Ideal college and he received his B.Sc(CS) from MR College, Peddapuram in the year 2015.

P.Radhika Krupalini is an Associate Professor of Computer Science Department at IDEAL COLLEGE OF ARTS AND SCIENCES, KAKINADAAP, INDIA. She passed M.Tech in Computer Science&Engineering from UCE,JNTU,Kakinada. She has Lectureship in Computer Science and Applications discipline and has an experience of 12 years of teaching.