A Secure Approach Using Existing Routing for Mobile Ad hoc Networks

[1] Koppolu Vijaya Lakshmi,[2]Srivyshnavi Pagadala.
[1]PG Student, Dept. of CSE, School of Engineering & Technology, Sri Padmavati Mahila University (Women's University), Tirupati.
[2]M.Tech (Ph.D),M.B.A,Assistant Professor, Dept. of CSE, Sri Padmavati Mahila University (Women's University), Tirupati .

Abstract: The flexibility and mobility of Mobile Ad hoc Networks (MANETs) have made them incrementing popular in a wide-range of avail cases. To forfend these networks, security protocols have been developed to forfend routing and application data .However, these protocols only forfend routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full bulwark. The utilization of communication security protocols pristinely developed for wire line and Wi-Fi networks can withal place a heftily ponderous encumbrance on the inhibited network resources of a MANET. To address these issues, a novel secure framework is proposed. The framework is designed to sanction subsisting network and routing protocols to perform their functions, whilst providing node authentication, access control, and communication security mechanisms. This paper presents a novel security framework for MANETs. The proposed frameworks felicitousness for wireless communication security.

Index Terms—access control, authentication, communication system security, mobile ad hoc networks.

INTRODUCTION

OBILE autonomous networked systems have optically discerned incremented utilization by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans. An example of an autonomous networked system is the Unmanned Aerial Conveyance (UAV). These can be diminutive-scale, networked platforms. Quadricopter swarms are an eminent example of such UAVs. Networked UAVs have concretely authoritatively mandating communication requisites, as data exchange is vital for the perpetual operation of the network. UAV swarms require conventional network control communication, resulting in frequent route changes due to their mobility. This topology generation accommodation is offered by a variety of Mobile Ad hoc Network (MANET) routing protocols [1].

MANETs are dynamic, self-configuring, and infrastructure- less groups of mobile contrivances. They are customarily engendered for a concrete purport. Each contrivance within a MANET is kenned as a node and must take the role of a client and a router. Communication across the network is achieved by forwarding packets to a destination node; when a direct source-destination link is unavailable intermediate nodes are utilized as routers. MANET communication is commonly wireless. Wireless communication can be trivially intercepted 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 manipulation attacks that can compromise the integrity of the network [2]. Eavesdropped communication may equip assailants with the expedient to compromise the trustworthiness of a network. This is achieved by manipulating routing tables, injecting erroneous route data or modifying routes. Man in the middle (MitM) attacks can be launched by manipulating routing data to pass traffic through malignant nodes [3]. Secure routing protocols have been proposed to mitigate attacks against MANETs, but these do not elongate bulwark to other data.

Autonomous systems require a paramount amount of communication [4]. Quandary solving algorithms, such as Distributed Task Allocation (DTA), are required to solve task orchestrating quandaries without human intervention. [4]As a result, these algorithms are vulnerably susceptible to packet loss and mendacious messages; partial data will lead to sub-optimal or failed task assignments.

This paper proposes a novel security protocol, Secure Routing for Mobile Ad hoc Networks. The protocol is designed to address node authentication, network access control, and secure communication for MANETs utilizing subsisting routing protocols. The routing and communication security at the network layer. This contrasts with subsisting approaches, which provide only routing or communication security, requiring multiple protocols to forfend the network. The remnant of this paper is organised as follows: Section II analyses the quandary in the context of antecedently published work. Section III introduces, providing a technical discussion of the protocol. Section IV outlines the characteristics culled for modelling, and the results of simulating this compared against culled secure routing and data security protocols. Section V draws conclusions from the research findings.

II RELATED WORK & PROBLEM ANALYSIS

A. MANET Routing

MANETs rely on intermediate nodes to route messages between distant nodes. Destitute of infrastructure to administrate the manner in which packets are routed to their destinations, MANET routing protocols instead make utilization of routing tables on every node in the network, containing either full or partial topology information. Reactive protocols, such as Ad hoc On-demand Distance Vector (AODV) [5], plan routes when messages need to be sent, polling nearby nodes in an endeavor to find the shortest route to the destination node. Optimised Link State Routing (OLSR) [6] takes a proactive approach, periodically flooding the network to engender routing table ingresses that persist until the next update. Both approaches are kineticism-tolerant and have been implemented in UAV MANETs [7], [8]. Kineticism-tolerance and cooperative communication characteristics make these protocols ideal for use in UAVs.

The fundamental versions of AODV and OLSR lack security mechanisms, sanctioning malignant nodes to interfere with the network in a variety of ways [9], [10], [11]. The key contributing factor to this quandary is an inability to distinguish legitimate nodes from malevolent nodes.

B. Security Threats

The ITU-T Rec., through X.805 [12], defines wireless endtoend security in seven relegations, which are called dimensions. This system of relegation sanctions for clear and convenient identification of security threats in a networks and potential solutions to those quandaries. The following security dimenstions are identified:

Access control is required to ascertain that malignant nodes are kept out of the network.

Authentication substantiates the identity of communicating nodes.

Non-repudiation averts nodes from broadcasting erroneous information about antecedent transmissions, mitigating replay and cognate attacks.

Confidentiality averts unauthorised nodes from deriving meaning from captured packet payloads.

Communication security ascertains that information only flows between source and destination without being diverted or intercepted.

Integrity checking sanctions nodes to ascertain packets received are in the same form they were sent, without modification or corruption.

Availability ascertains that network assets are accessible. Periodic checking of node status or reports from a node to its neighbours are a mundane denotes of checking the availability of a resource.

Privacy obviates outside observers from deriving valuable information through passive observation.

Many MANET routing protocols surmise trust between nodes, which can be a critical impuissance in terms of security [9], as such a postulation may sanction malevolent nodes to interfere with routing mechanisms. Routing attacks can abuse the route revelation and topology generation much mechanisms of routing protocols. An assailant could, for example, advertise routes with hop counts higher or lower than authentic routes [13]. This could be acclimated to magnetize traffic to malignant nodes to the benefit of the assailer. Malignant activity may result in; the appropriation of data, sinking of packets and modification of packets. All such outcomes impair the networks competency to assure safe, private and reliable communication.

Unsecured pro-active routing protocols exhibit susceptibility to packet replay and manipulation attacks [14]. Due to a lack of source authentication, topology control messages can be broadcast frequently, which other nodes will treat as legitimate and use to update ecumenical topology information. Proactive routing protocols detect neighbours through HELLO messages, sanctioning tunnelling attacks if a malignant intermediate node reports a route between two out of range nodes [15]. This results in the construction of a mendacious topology, causing failure of the network when endeavoring to utilize incorrectly advertised routes.

Packet forwarding attacks may be utilized for Denial of Accommodation (DoS). These assailments do not target the routing protocol, instead coercing the node in the network to act in a manner inconsistently erratic with the routes established, engendering an excess of traffic or sinking packets malevolently [16]. X.805 describes five key threats [12]:

- Ravagement: Consummately abstracting a packet from thenetwork and expunging it locally, obviating it from reachingdestination and ravaging the packet
- Corruption and modification: Making a packet unreadable,or transmuting the content of the packet
- Larceny, loss or abstraction: Glomming packets from the networkfor further analysis, causing packets to drop or removingthem from the network
- Disclosure: Revealing network information by re-broadcastingreceived packets to untrusted nodes
- Interruption of accommodations: Disruption of any accommodation thenetwork offers, resulting in loss of accommodation or unacceptable completion time.

Yang et al. notes that maleficent attacks may facilely disrupt MANET operations [9]. An assailant can capitalize on MANETs that surmise, but not enforce, trust between

nodes. Closing the network by coercing legitimate nodes to authenticate can resolve the postulation of trust, by ascertaining that only legitimate nodes can become members

of the network [17]. In a closed network, participation is restricted to sanctioned nodes, and communication is encrypted to obviate third-party comprehension of the contents of network communication.

Authentication is required to sanction incipient nodes to join and be optically discerned as legitimate by

subsisting network members [18]. The duration an individual UAV node may remain operational is inhibited by its battery life (energy), which may be shorter than the expected duration of the network's deployment [19]. A supersession may be required
if a node runs out of energy.

Malignant nodes may masquerade as legitimate nodes, endeavoring to gain trusted status in the network by posing as a recently departed
or incipiently arriving node [10]. Subversion of the supersession procedure may be mitigated
by requiring the prosperous authentication of a node. with the network. This approach would authenticate nodes utilizing cerfitificates provided at initialisation by a trusted ascendancy. This ascendancy is central to the networksecurity scheme, but need not be present in the field [18].

2.3 MANET Routing Security To tackle the quandaries that surmised legitimacy can cause, secure MANET routing protocols have been proposed. SecureAd hoc On-demand Distance Vector (SAODV) andSecure Optimised Link State Routing (SOLSR) are secureimplementations of AODV and OLSR respectively.SAODV secures the routing mechanism by including arbitrary numbers in Route Request packets (RREQs) [20]. If a routing packet arrives that re-utilizes an old packet number, that packet is invalid. Nodes observed sending re-played packets may be flagged as malevolent.

SAODV requires that at least two Secure RREQs (SRREQs) arrive at the destination node by different routes with identical desultory numbersto identify the source node. SOLSR aims to sanction detection of wormhole attacks during its neighbor detection phase [14]. Nodes should be authenticated prior to establishing neighbor status to avert malevolent nodes from asserting themselves as neighbours. Verification of a source node's identity must be performed. Each node is surmised to have an asymmetric key pair, managed by a coalition of nodes utilizing thresholdcryptography.

A distributed Certificate Ascendancy (CA) system is required to manage this process if certificates are superseded in the field. Each packet sent by SOLSR is digitally signed utilizing a shared secret. If an incoming packet’s signature is unreadable, the packet is discarded as being unauthentic. This is a point-to-point process and does not provide source authentication.
To prevent replay attacks, SOLSR uses timestampedpackets. If a time-stamp is seen twice by a legitimatenode, the packet will be discarded [14], [15].Due to the lower hardware specifications and resourcerestrictions on UAV-based MANETs, the use of individualnodes as authentication servers is not ideal. If a node iscompromised, it may deny legitimate nodes access to thenetwork. If a compromised node has authentication privileges,it may authenticate additional malicious nodes andpossibly blacklist legitimate nodes.
Centralized approaches rely on a single node takingcontrol of key management and trust systems [21]. Thisputs additional strain on that node due to repeated call forauthentication from other nodes. It also presents a singlevector of attack against network security mechanisms; if
the central authority is compromised; the entire networkmay also be compromised.
The primary objective of SAODV and SOLSR is to preventmalicious nodes from gaining control of the topologygeneration mechanisms of the routing protocol, and to protectagainst black hole and wormhole attacks. Routing issecured and malicious node detection is employed in bothcases.

IIIFRAMEWORk

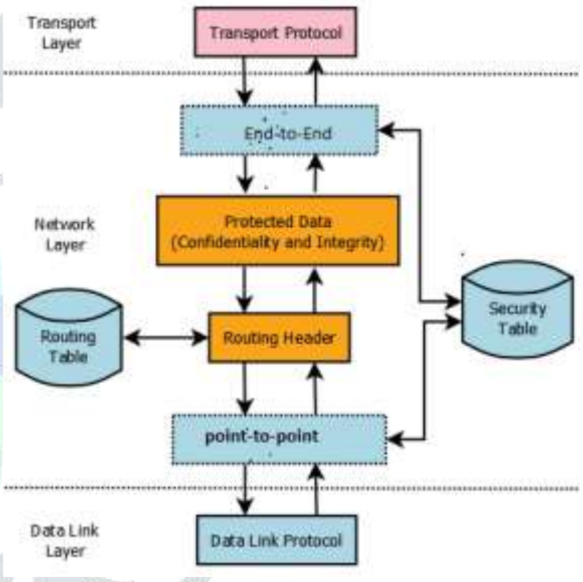


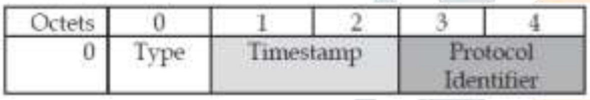
Fig.1. Diagram illustrating the confidentiality, integrityand authentication services for data packets

It is a framework that operates at the networklayer (layer 3) of the OSI model. It is designed to provide afully secured communication framework for MANETs,without requiring modification of the routing protocol.Fig. 1 shows the flow of data from transport, through thenetwork layer to the data linklayer. The dashed boxes represent elements of that process packets and

Trusted Authority (TA)o A static node responsible for node initialisation and provision of certificates. Required per node and shared with other nodes to jointhe network. Public Diffie-Hellman Key Share (*DKSp*) A public value communicated between nodes. Private Diffie-Hellman Key Share (*DKSpriv*)A private value, held by all nodes in the network andnever communicated.
Used as the shared secret for Diffie-Hellman key exchangeIdentifier (I)o A per node unique identifier, such as an IP address in anIP-based networkEncrypted Payload (EP)o Payload data encrypted using an encryption

schemesuch as AEAD Tag (T)o A tag, appended as a footer to all packetsto provide point-to-point integrity services Symmetric key (SK)o *SKe(s,d)* is a security key used for encryption of end-to-endcommunication between a source and destinationnode, derived locally via KDF from the product of the*DKSp* and *DKSpriv*
o *SKp(s,d)* shared by two nodes; used to authenticate trafficas it moves along the network, derived locally viaKDF from the product of the *DKSp* and *DKSpv* Key Derivation Function (*KDF(SK,func)*)o A function used to provide multiple different keys froma common private source. Symmetric broadcast key (*SKb*), shared with newcomernodes by the node that allows them to join the network,generated by the first node to initialize the network. Differentiated into two application specific keys by a networkwideKDF stored locally on each nodeo Symmetric end-to-end broadcast key (*SKbe*)o Symmetric point-to-point broadcast key (*Skbp*)

A. Framework Overview It packet shares a common packet header (H), shown in Fig. 2. The data contained inthe header can be broken down as follows: Packet Type denotes the function of the packetTimestamps provide uniqueness, allowing detection of replayedpackets and providing a basis for non-repudiation ofpreviously sent packets□ The protocol identifier indicates the layer 4 type of the encapsulateddata. This would be the IP protocol number inan IP based network.



Octets	0	1	2	3	4
0	Type	Timestamp		Protocol Identifier	

Fig. 2. Packet Header (H) structure

Key Management

This paper relies on the dynamic generation of keys toprovide secure communication.The Diffie-Hellman key-exchange algorithm provides ameans of generating symmetric keys dynamically and isused to generate the SK keys. *SKb* keys can simply be generatedby means of random number generation or anequivalent secure key generation service.*Secure Node-to-N*

*ode Keys**SKe* keys are used to secure end-to-end communicationwith other nodes, with one *SKe* key generated per node, forevery other node also authenticated with the network. *SKp*keys are used for point-to-point security and generated inthe same manner as *SKe* keys.It is important that *SKe* and *SKp* keys are different, asthe network needs to secure both the content of a packetand the route taken.

A KDF can be used to generate these two keys in conjunctionwith the result of the Diffie-Hellman algorithm,requiring a *DKSp/DKSpriv* pair, to minimise the cost of securityon the network and reduce the key re-use and, inturn the lifetime of each key.These keys are generated when nodes receive DKSp'sfrom other nodes.

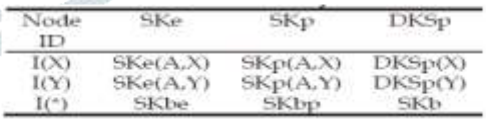
*Secure Point-to-Point Footers*Secure footers are appended to all communication packetssent between the nodes. *SKbp* and *SKp(x)* keysare used in broadcast and unicast integrity service provisionrespectively.

*Secure Broadcast Keys*At initialisation of the network, the first node to be contactedabout joining the network will generate a symmetricnetwork key (*SKb*). This key is sent to all nodes that authenticatewith the network.The *SKb* is processed by the function *KDF(SKb, type)* intotwo broadcast keys (*SKbe* and *SKbp*).A node will use these keys to encrypt and sign packetssent to the broadcast address of the network.

This key isused for broadcast and multicast communication, such asMANET route updates. It is not used for communicationbetween individual end-points.Upon deriving a broadcast keythat will be tied to thenetwork, the receiving node will add the resulting keys toits security table. *SKbe* keys are used to provide confidentialityto end-to-end broadcast communication. *SKbp* keysare used to generate tags, generated using an algorithmsuch as HMAC, as a footer to protectedpackets, providing broadcast packet integrity.Broadcast keys are generated by the first node to participatein a network joining process as the authenticator (theresponding partner). They are then shared as the finalstage of all network joining processes that result in a newnode becoming a part of that network.

*Storage*stores keys in each node's security table. Thesecurity table contains the security credentials of nodes with which the node has previously directly communicated,as shown in Table 1. This table has *n* entries, where*n* is the number of nodes that the node in question has directlycommunicated with. Table 1 shows an example of asecurity table belonging to node A. It has exchanged credentialswith two other nodes, X and Y.

TABLE 1
Security Table

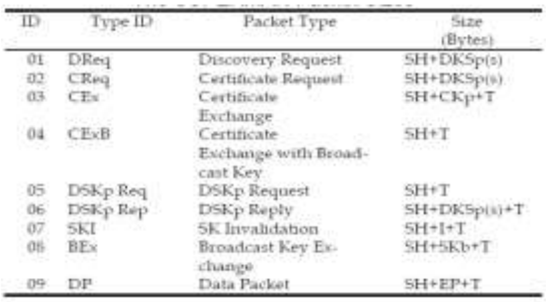


Node ID	SKe	SKp	DKSp
I(X)	SKe(A,X)	SKp(A,X)	DKSp(X)
I(Y)	SKe(A,Y)	SKp(A,Y)	DKSp(Y)
I(*)	SKbe	SKbp	SKb

The shared symmetric broadcast key (*SKb*) has two derivedforms, the *SKbe* and *SKbp*. These are stored in the localsecurity table as a separate broadcast address, denotedby I(*). These keys are not associated with any one network,but represent security credentials held by the wholenetwork. A node's ID would be its address.

TABLE 2

Packet Types



ID	Type ID	Packet Type	Size (Bytes)
01	DReq	Discovery Request	SH+DKSp(s)
02	CReq	Certificate Request	SH+DKSp(s)
03	CEx	Certificate Exchange	SH+CKp+T
04	CExB	Certificate Exchange with Broad-cast Key	SH+T
05	DSKp Req	DSKp Request	SH+T
06	DSKp Rep	DSKp Reply	SH+DKSp(s)+T
07	SKI	SK Invalidation	SH+I+T
08	BEx	Broadcast Key Exchange	SH+SKb+T
09	DP	Data Packet	SH+EP+T

Table 2 shows the packet types used to includingtheir default packet sizes before the addition ofany network layer headers such as IP or data link layerheaders such as 802.11.

IV METHODOLOGY AND RESULTS

To analyse, the following key areas were investigated:Comparison of security dimension coverage Number of communication events required to secure communicationsbetween all nodesNumber of bytes required to secure communications betweenall nodesOverhead of securing communication required for routegenerationOverhead of securing communication required by ConsensusBased Bundle Algorithm (CBBA) and ClusterForm CBBA (CF-CBBA)The eight key security dimensions, outlined in X.805 areevaluated by comparison between SAODV,SOLSR, and IPsec/MANIPsec.

These are compared interms of the services provided. This is important becauseit contextualizes the comparisons of the respective securityand communication costs.These costs represent the additional data or packets(based on the number of communication events) required

to provide the security services, referred to from this pointas the security overhead.Overheads are calculated for the network layer of theOSI model. The Datalink and Physical layers of the networkstack are not considered as this paper focuses on thenetwork layer (OSI layer 3) specifically.

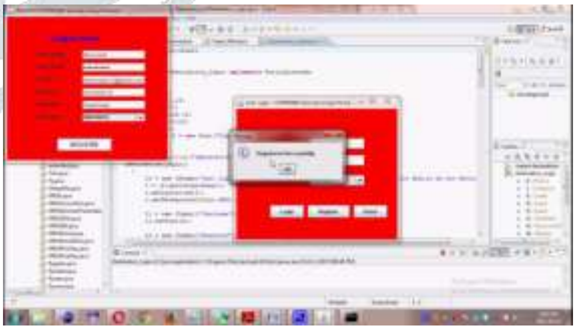
All simulation is performed using JAVA. shows the parameters for the simulation environment.It is assumed that all packets arrive intact without bit-erroror loss, and that nodes are stationary during the initialization and association phases.

JAVA was chosen as simulation tool. Pre-existingCBBA simulation code has been used as a core for the DTAscenarios selected for these experiments, resulting in thenetwork simulation being built alongside the DTA simulation.Network communication was simulated assuming perfectconditions (no loss unless introduced experimentally).The authors rationalize that a proportional increase incommunication cost, if observed under identical channelconditions, will remain proportional between the comparedprotocols regardless of the underlying conditions. As thisis a comparative exercise, the assumption of a perfectchannel is appropriate.

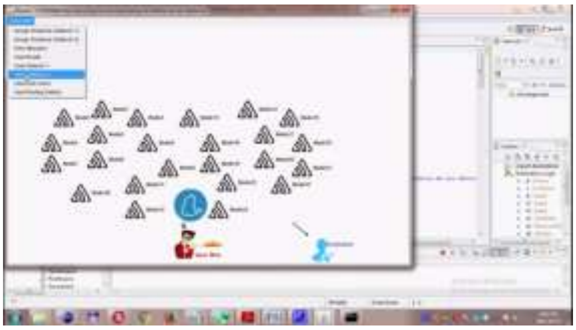
Source

DESTINATION-1

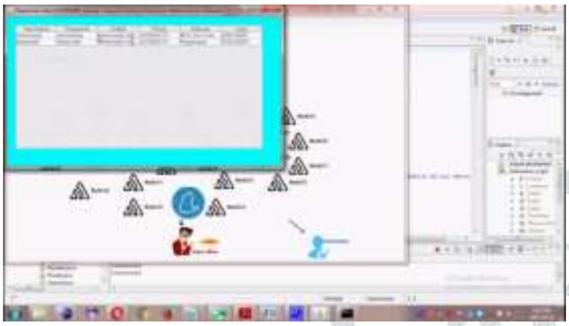
USER REGISTER



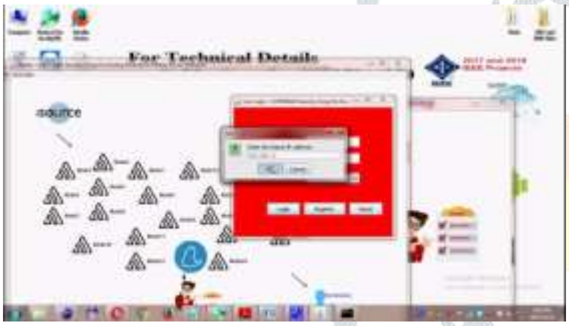
ROUTER

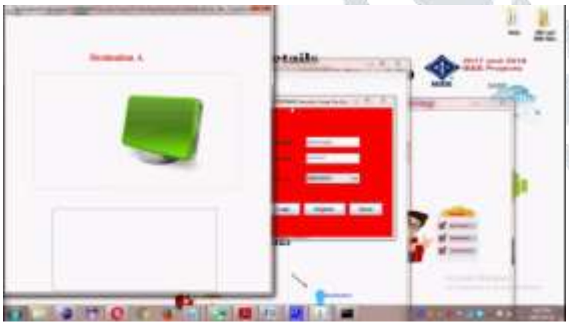


VIEW USERS

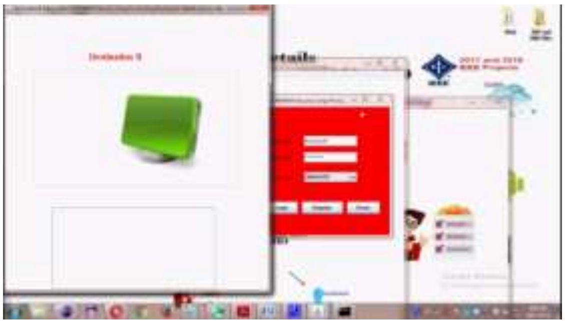


DESTINATION LOGIN

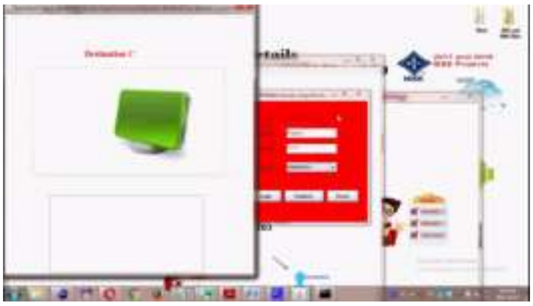




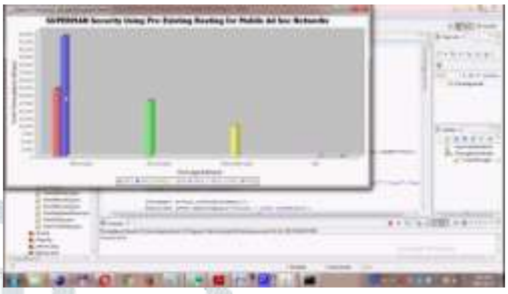
DESTINATION-B



DESTINATION-C



GRAPH



V CONCLUSIONS

It is a novel security framework that bulwarks the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that sanctions expedient, reliable communication with confidentiality, integrity and authenticity accommodations. addresses all eight security dimensions outlined in X.805. Thus, can be verbally expressed to implement a full suite of security accommodations for autonomous MANETs. It consummates more of the core accommodations outlined in X.805 than IPsec, due to being network focused in lieu of end-to-end oriented. By obviating the ingress of potentially untrustworthy nodes to the network, and thus the routing process, a MANET may be bulwarked from subversion of its routing accommodations at a lower cost, as malevolent nodes are barred from the process entirely.

This will be provides security to all data communicated over a MANET. It concretely targets the attributes of MANETs, it is not felicitous for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ascertain that MANET communication is bulwarked consummately and efficiently. A single efficient method bulwarks routing and application data, ascertaining that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes. Future work includes the implementation of a simple mobile node platform to sanction experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing accommodations between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on to better understand the role of the credential referral mechanism on overhead mitigation in networks.

REFERENCES

[1] P. S. Kiran, “Protocol architecture for mobile ad hocnetworks,” *2009 IEEE International Advance ComputingConference (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, “Differenttypes of attacks on integrated manet-internet communication,”*International Journal of Computer Scienceand Security*, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherill, S. Woodhead, and A. Adekunle,“A cluster-based approach to consensus baseddistributed task allocation,” in *Parallel, Distributed andNetwork-Based Processing (PDP), 2014 22nd EuromicroInternational Conference on*. IEEE, 2014, pp. 428–431.

[5] I. D. Chakeres and E. M. Belding-Royer, “Aodv routingprotocol implementation design,” in *DistributedComputing Systems Workshops, 2004. Proceedings. 24thInternational 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.*, “Optimizedlink state routing protocol (olsr),” 2003.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A.Temple, “Simulation-based performance evaluation ofmobile ad hoc routing protocols in a swarm of unmannedaerial vehicles,” in *Advanced Information Networkingand 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, “Performanceanalysis of mesh routing protocols for uav swarmingapplications,” in *Wireless CommunicationSystems (ISWCS), 2011 8th International Symposium on*.IEEE, 2011, pp. 317–321.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Securityin 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, “Anevaluation 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 securityassessment and planning,” in *TelecommunicationsNetwork Strategy and Planning Symposium. NETWORKS2004, 11th International*. IEEE, 2004, pp. 273–278.

[13] M. G. Zapata, “Secure ad hoc on-demand distancevector routing,” *ACM SIGMOBILE Mobile Computingand Communications Review*, vol. 6, no. 3, pp. 106–107,2002.

[14] F. Hong, L. Hong, and C. Fu, “Secure olsr,” in *AdvancedInformation 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] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, “Dos attacksin mobile ad hoc networks: A survey,” in *AdvancedComputing & Communication Technologies (ACCT), 2012 Second International Conference on*. IEEE,2012, pp. 535–541.

[17] S. Maity and S. K. Ghosh, “Enforcement of access controlpolicy for mobile ad hoc networks,” in *Proceedingsof the Fifth International Conference on Security of Informationand Networks*. ACM, 2012, pp. 47–52.

[18] D. Hurley-Smith, J. Wetherall, and A. Adekunle, “Virtualclosed networks: A secure approach to autonomousmobile ad hoc networks,” in *2015 10th InternationalConference for Internet Technology and SecuredTransactions (ICITST)*. IEEE, 2015, pp. 391–398.

[19] S. Bhattacharya and T. Basar, “Game-theoretic analysisof an aerial jamming attack on a uav communicationnetwork,” in *American Control Conference (ACC),2010*. IEEE, 2010, pp. 818–823.

[20] S. Lu, L. Li, K.-Y. Lam, and L. Jia, “Saodv: a manetrouting 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 managementand secure routing integrated framework formobile ad-hoc networks,” *Ad Hoc Networks*, vol. 11,no. 3, pp. 1046–1061, 2013.

[22] M. Myers, R. Ankney, A. Malpani, S. Galperin, andC. Adams, “X. 509 internet public key infrastructureonline certificate status protocol-ocsp,” RFC 2560,Tech. Rep., 1999.

[23] N. Doraswamy and D. Harkins, *IPSec: the new securitystandard for the Internet, intranets, and virtual private networks*.Prentice Hall Professional, 2003.

[24] A. Ghosh, R. Talpade, M. Elaoud, andM. Bereschinsky, “Securing ad-hoc networks using ipsec,”in *Military Communications Conference, 2005. MILCOM2005. IEEE*. IEEE, 2005, pp. 2948–2953.

[25] K. N. Ali, M. Basheeruddin, S. K. Moinuddin, andR. 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] E. Rescorla, "Diffie-hellman key agreement method,"1999.

[27] L. Harn, M. Mehta, and W.-J. Hsin, "Integrating diffiehellmankey exchange into the digital signature algorithm(dsa)," *Communications Letters*, *IEEE*, vol. 8,no. 3, pp. 198–200, 2004.

[28] H. Krawczyk and P. Eronen, "Hmac-based extractand-expand key derivation function (hkdf)," 2010.

[29] A. Adekunle and S. Woodhead, "An aead cryptographicframework and tinyaead construct for securewsn communication," in *Wireless Advanced (WiAd),2012*. IEEE, 2012, pp. 1–5.

Koppolu Vijaya Lakshmi was born in AP, India. Currently she is studying her Post graduate degree in School of Engineering & Technology, Sri PadamavathiMahilaVisvaVidhyalayam, Tirupathi in Department of Computer Science & Engineering.

Sri Vyshnavi Pagadala is currently working as an Assistant Professor in CSE department, School of Engineering & Technology, Sri PadamavathiMahilaVisvaVidhyalayam,Tirupati.