Security Using Enhancement of Diffie-Hellman algorithm for Mobile Ad hoc Networks

[1] S. Navya

[1] Assistant Professor in Computer Science and Engineering at Raghu Engineering College, Dakamarri, Visakhapatnam, India

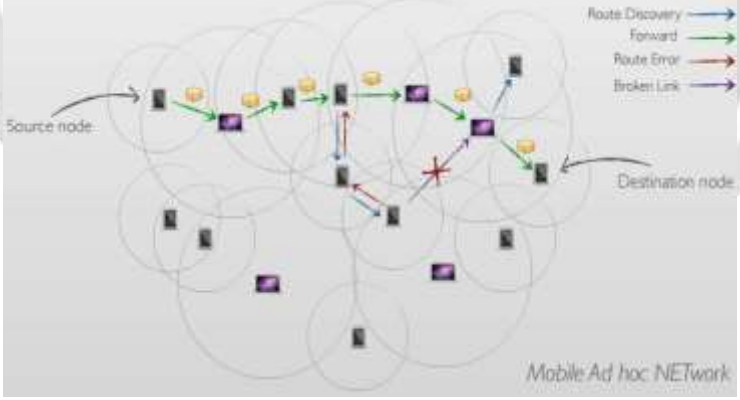
ABSTRACT

Mobile Ad hoc Networks (MANETs) have increased their popularity across a wide range of applications. To protect those networks, routing security approaches and awareness statistics were established. Using the current system, a strong framework was added. These current protocols are designed to create stable routes between nodes by utilising presenting safety for give-to-give up and factor-to-factor verbal exchange for the sole purpose of course discovery. We've pushed the Diffie-Hellman set of rules to the next level because statistics exchanged over such channels aren't always consistent. I added the idea of using the Diffie-Hellman set of rules to build a more powerful mystery key, which is then sent between the sender and recipient

Keywords— *Access control, authentication, communication system security, MANETS, Diffie-Hellman*

1 Introduction

A Mobile Ad-hoc Network (MANET) is a self-organizing and self-configuring multi-hop wireless network with a dynamic network structure. This is primarily owing to the nodes' mobility. To communicate with the other nodes in the MANET, each node employs a wireless interface. These networks are completely distributed and can function in any location without the need for any established infrastructure. Nodes can communicate with one another fast within the radio range. Intermediate nodes, which relay packets from source to destination, can connect nodes that are not within radio range of one other. The advantage of the manet is that it is ideal for temporary network setups. The MANET has the drawbacks of being less secure and having topologies that change frequently..



1.1 DSR(Dynamic Source Routing):

The Dynamic Source Routing (DSR) protocol is a source-based on-demand routing technology. The DSR Protocol is made up of two “on-demand” mechanisms that are activated only when two nodes desire to communicate..

Advantages

The route is created only when it is required and the node utilize the route cache information efficiently to reduce the overhead and collision

Disadvantages

The route Maintenance mechanism does not locally repair a broken link. The delay is higher than in **table-driven protocols.**

2. Literature Review

2.1 MANET Routing:

Messages between distant nodes are routed through intermediate nodes in MANETs. Due to a lack of infrastructure to manage how packets are routed to their destinations, MANET routing protocols rely on routing tables on each node in the network, which include either complete or partial topological information. When messages need to be conveyed, reactive proto- cols like Ad hoc On-demand Distance Vector (AODV) [5] create routes by polling adjacent nodes in an attempt to discover the quickest path to the destination.

Optimized Link State Routing (OLSR) [6] employs a proactive approach, flooding the network on a regular basis to generate routing table entries that last until the next update. Both methods are motion-tolerant, and they have been used in UAV MANETs [7], [8]. These proto- cols are suited for use in UAVs because of their motion-tolerance and cooperative communication capabilities.

AODV and OLSR's basic versions lack security features, allowing hostile nodes to disrupt the network in a number of ways [9], [10], [11]. The inability to identify legitimate nodes from malicious nodes is a major contributing cause to this problem.

2.2 Security Threats:

The ITU-T Rec. X.805 [12] divides wireless end-to-end security into seven categories, which are referred as as dimensions. This classification method enables quick and easy identification of security threats in a network, as well as viable remedies to such problems. The following security parameters have been identified:

Access control is required to ensure that malicious nodes are kept out of the network.

- ✓ Authentication verifies that communication nodes are who they say they are.
- ✓ Non-repudiation protects against replay and other attacks by preventing nodes from broadcasting incorrect information about prior transmissions.
- ✓ Unauthorized nodes are unable to derive meaning from collected packet payloads due to confidentiality..
- ✓ Communication security ensures that only Flows between source and destination without being deflected or intercepted; approved individuals have access to information. Nodes use integrity checking to ensure that packets received are in the same state as when they were transmitted, with no alteration or corruption.

The availability of network assets ensures that they can be accessed. Checking node status or reports from a node to its neighbours on a regular basis is a typical way to ensure that a resource is available. Outside observers are unable to derive valuable information from passive observation due to privacy.

Many MANET routing protocols presuppose node trust, which can be a security flaw [9], since such an assumption may allow hostile nodes to communicate with each other.

to cause routing mechanisms to be disrupted. Routing attacks can take advantage of routing protocols' route discovery and topology generation techniques. For example, an attacker might advertise routes with larger or lower hop counts than actual routes [13]. This could be exploited to direct traffic to malicious nodes for the attacker's benefit. Data appropriation, packet sinking, and packet manipulation are all possible outcomes of malicious action. All of these results jeopardise the networks' ability to ensure secure, private, and dependable communication..

Packet replay and manipulation attacks are vulnerable to unsecured proactive routing protocols [14]. Topology control messages can be broadcast often due to a lack of source authentication, which other nodes will perceive as legitimate and utilise to update global topology information. Proactive routing methods use HELLO messages to detect neighbours, allowing tunnelling attacks if a router is compromised.

A path between two out-of-range nodes is reported by a rogue intermediate node [15]. As a result, a fake topol- ogy is built, leading the network to fail when attempting to use improperly advertised routes.

Denial of service attacks can be carried out using packet forwarding (DoS). These attacks do not target the routing protocol; instead, they force nodes in the network to operate in ways that are incompatible with the routes that have been established, resulting in excessive traffic or intentional packet sinking [16]. Five major risks are described in X.805 [12]:

- ✓ Destruction: Taking a packet off the network and erasing it locally, preventing it from reaching its destination and effectively destroying it. Modification and corruption: Making a packet unreadable or altering the packet's content
- ✓ Stealing packets from the network for further analysis, forcing packets to drop, or deleting them from the network are all examples of theft, loss, or removal.
- ✓ Re-broadcasting incoming packets to untrustworthy nodes to reveal network information.

- ✓ Interruption of services: Any of the network's services is disrupted, resulting in a loss of service or an unacceptable completion time.

Malicious attacks, according to Yang et al. [9], can readily disrupt MANET functioning. MANETs that assume but do not enforce trust between nodes can be exploited by an attacker. Closing the network by requiring valid nodes to authenticate can resolve the trust assumption by ensuring that only legitimate nodes can join the network [17]. Participation in a closed network is limited to permitted nodes, and communication is encrypted to prevent third-party understanding of network communication. To allow new nodes to join and be recognised as valid by current network members, authentication is necessary [18].

The battery life (energy) of a single UAV node limits the period of time it can stay active, which may be less than the network's anticipated rollout timeline [19]. It may be required to replace a node if it runs out of energy. Malicious nodes can spoof legitimate nodes to gain network trust by posing as a just arrived or recently departed node [10].

Subversion of the replacement operation can be mitigated by requiring a node's authentication with the network to be successful. This method would authenticate nodes by using certificates given by a trusted authority at the time of initialization. Although this authority is critical to the network security architecture, it is not required to be present in the field [18].

2.3 MANET Routing Security:

Secure MANET routing techniques have been developed to address the issues that presumed validity can cause. SAODV (Secure Ad hoc On-demand Distance Vector) and SOLSR (Secure Optimised Link State Routing) are secure AODV and OLSR implementations, respectively. By inserting random numbers in Route Request packets (RREs), SAODV secures the routing mechanism [20]. If a routing packet arrives with an old packet number, it is invalid. Nodes that send re-played packets may be considered malicious. To identify the originating node, SAODV needs that at least two Secure RREs (SRREs) arrive at the destination node over distinct routes with identical random numbers.

During its neighbour discovery phase, SOLSR seeks to detect wormhole attacks [14]. To prevent rogue nodes from claiming to be neighbours, nodes should be authenticated before establishing neighbour status. It is necessary to verify the identification of a source node. Each node is supposed to have an asymetric key pair, which is maintained using threshold cryptography by a coalition of nodes. If certificates need to be replaced in the field, a distributed Certificate Authority (CA) system is necessary to oversee the process.

SOLSR uses a shared secret to digitally sign each packet it sends. If the signature on an inbound packet cannot be read, the packet is deleted as unauthentic. This is a one-way process that doesn't give source authentication. SOLSR employs time-stamped packets to prevent replay attacks. If a legitimate node sees a time-stamp twice, the packet is rejected [14], [15]..

Individual nodes as authentication servers are not appropriate in UAV-based MANETs because to lower hardware specifications and resource constraints. If a node is com- promised, genuine nodes may be denied access to the network. If a compromised node has authentication credentials, it may be able to authenticate more malicious nodes while also blacklisting legal nodes.

The control of key management and trust systems is delegated to a single node in centralised techniques [21]. As a result, extra burden on that node as a result of repeated authentication requests from other nodes It also exposes a single attack vector against network security procedures; if the central authority is compromised, the entire network could be compromised as well.

The major goal of SAODV and SOLSR is to protect against black hole and By preventing malicious nodes from gaining control of the routing protocol's topology formation algorithms, wormhole attacks can be avoided. Routing is secured in both circumstances, and malicious node detection is used.

2.4 Secure Communication:

Securing pathways is only one part of a comprehensive security strategy. Many security dangers are highlighted in X.805, including identity theft, data tampering, corruption, and theft [12]. Authentication, secrecy, and integrity are the three elements for securing communication. X.509 is the industry standard for certificate-based security [22]. Certificates are a collection of data that can be used to describe a node's identity and its relationship with a trusted authority.

IPsec (Internet Protocol Security) is a secure communication architecture that provides secrecy, integrity, and authentication. Authentication Headers (AH), Encapsulating Security Payloads (ESP), and Security Associations (SA) are the three fundamental protocols [23].

Connectionless integrity and source authentication are provided by AH. Because IPsec does not account for the route taken to the destination, it does not provide route authentication.
ESP offers services such as secrecy, integrity, and authentication. ESP does not provide protection to a packet's IP header. When the IP header must be exchanged, such as during multi-hop activities, this is advantageous. Once the IP headers have been deleted, ESP encapsulates an AH packet that offers source authentication.
SA is a set of security features that AH and ESP both use. To offer a common base for encryption, authentication, and integrity checking, all nodes in the network share a SA.
Ghosh et al. [24] discuss how to modify an IPsec certificate-based application to accommodate dynamic key generation for MANETs. Their method ensures mobility, application, and management traffic, according to them. They reported increased latency and bandwidth utilisation as a result of their methods.
MANIPsec [25] is a model that is solely focused on MANET security with IPsec. They offer a modified IPsec protocol. Lightweight security was prioritised while authentication and confidentiality were maintained. Their concept aims to make all control traffic, including routing traffic, secure. When compared to most application-driven traffic, network control traffic, such as routing activities, requires significant resources, according to their findings.
To this point, all of the choices have depended on certifi- cates for security. The certificate can be used to generate symmetric keys for secure communication, allowing for the extension of secrecy, integrity, and authentication services to any packets that require them.

3 Proposed Method

The Diffie-Hellman key generation technique is an example of a method for creating symmetric keys without the need to disclose sensitive key information explicitly [26]. Nodes use globally known primes and local secret data to exchange locally created data. Both nodes then transmit the resulting variable (referred to as a key-share), allowing for the generation of a symmetric key that is identical on both ends without requiring sensitive data to be sent at any moment. This makes it possible to establish discrete and secure node-to-node secrecy between certain node pairs [27].
Multiple keys can be created from a single source key and meta-data using key derivation functions (KDF) [28]. This is useful when a single shared secret needs to be utilised in multiple places.

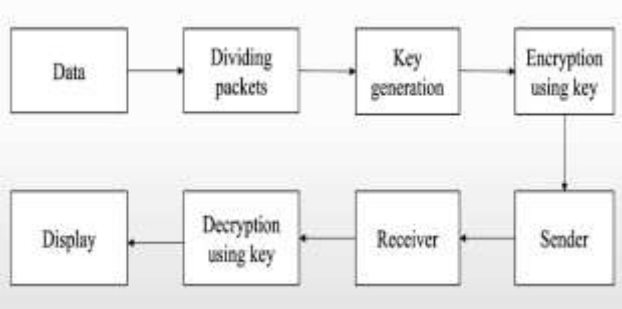


Fig 1:- Module diagram with input and output information

4 Proposed Algorithm

Enhance Diffie-Hellman Algorithm
Sender and Receiver agree on a prime number p, q as it's primitive root. Their
choose private key 'a' and 'b' which is known to themselves only.
Sender's public key A= q^a mod p.
Receiver's public key B= q^b mod p.
Sender and Receiver exchange their public key. Now Sender has B and Receiver has A.
Sender calculates
B^a mod p= q^bamod = S.
Receiver calculates
A^b mod p= q^ba mod p =S.

Hence, the sender and receiver get 'S' as their shared secret key.

Now, Sender and Receiver take ‘e’ as the primitive root of ‘S’.
Sender and Receiver generate their own so called private key ‘f’ and ‘g’ which is known to themselves. Sender’s

Second public key C= e^f mod S.
Receiver’s second public key D= e^g mod S.

Sender and Receiver exchange their second public key. Now Sender has D and Receiver has C. On the basis of second public keys and so called private keys, sender and receiver will now calculate their second shared-secret key (W) which is same to both.

SECOND SHARED SECRET KEY (W):

Sender calculates Df mod S= e gf mod S= W.
Receiver calculates Cg mod S= e fgmod S= W.

Hence, the sender and Receiver get ‘W’ as their second shared-secret key.
Sender and Receiver select their random number ‘h’ and ‘i’.
Sender calculates: X= (W*h) and Receiver calculates: Y= (W*i) Sender and Receiver exchange X and Y finally.
The sender and receiver get a shared-secret key by using the existing Diffie- Hellman algorithm, now they find the primitive root of their shared-secret key. Using the Diffie-Hellman algorithm for the second time and sender and receiver will get a second-secret key.

HMAC tag:

- ✓ Hash – based message authentication code is a mechanism for calculating a message authentication code involving hash function in combination with a secret key.
- ✓ This is used to verify the integrity and authenticity of a message. HMAC tag is applied to the entire packet to provide point to point integrity.
- ✓ A tag is generated using the shared key of the transmitting node and next hop. The tag is replaced at each intermediate hop, until the destination node is reached. Thus, the authenticity of a route is maintained, as each node on the route must prove their authenticity to the next hop. This tag can also be used for integrity checking.
- ✓

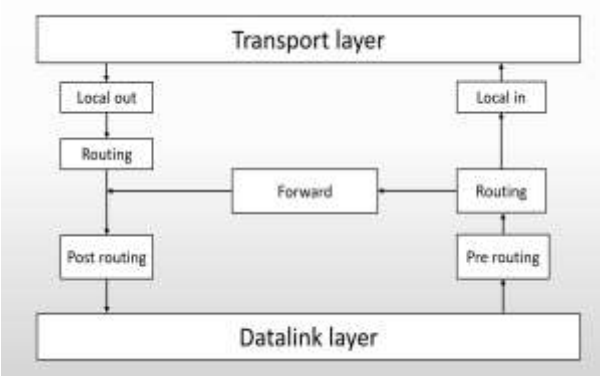


Fig 2 :-System Architecture

5 METHODOLOGY:

PERFORMANCE METRIC

Throghput: The throughput is the measure of how fast we can actually send data through the network. It is the measurement of number of packets that are transmitted through the network in a unit of time. The performance is better when throughput is high.

$$\text{Throughput} = \frac{totalnumberofbyterecived}{totaltimeoftransmission}$$

Packet Delivery Ratio: Packet Delivery Ratio is a ratio of number of packets received at the destination nodes to the number of packets send from the source nodes. The performance is better when packets delivery ratio is high.

$$\text{Packet Delivery Ratio} = \frac{totalnumberofrecivedpackets}{totalnumberoftransmittedpackets}$$

End-to-End Delay: End-to-End delay is a average time delay for data packets from the source node to the destination node. To find out the end-to-end delay the difference of packet sent and received time was stored and then dividing the total time difference over the total number of packet received give the average end-to-end delay for the received packets. The performance is better when packet end-to-end delay is low.

$$\text{End to End Delay} = \frac{\sum(arrivetime - sendtime)}{totallnumberoftransmitpacket}$$

6 SIMULATION RESULTS:

Simulation Parameter	Value
Simulation	NS2-2.34
Routing Protocol	AODV, DSR
Channel Type	Wireless channel
Number nodes	50
Traffic Type	CBR
X axis distance	2200
Y axis distance	970
MAC Type	802.11
Max packet	300

Table 1:- simulation parameters taken in the proposed system

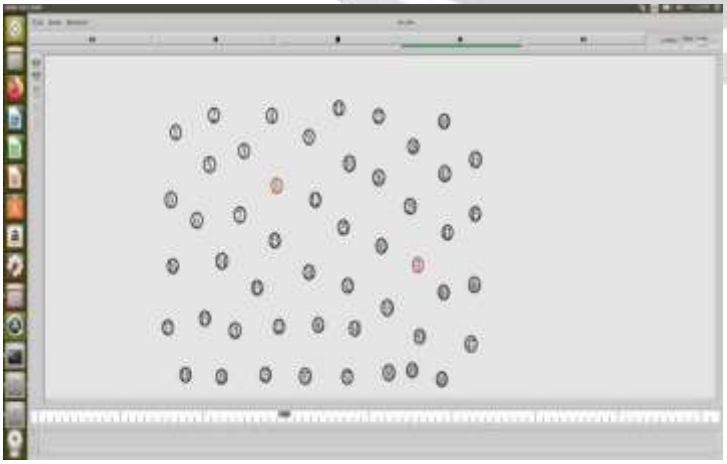


Fig 3:- Verifying each neighbouring node in the transmission range from node 8 to node 31 in the network and finds the path. Node 8 is source and node 31 is Destination node

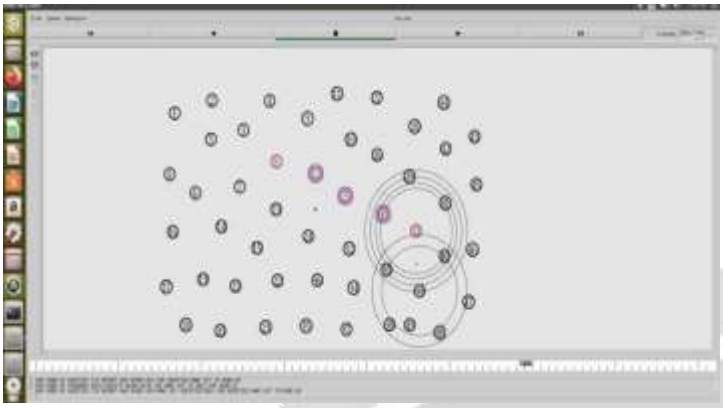


Fig 4:- Eavesdrop Attacker is detect at node 49 after verifying node 31 with the neighbouring nodes in the transmission range

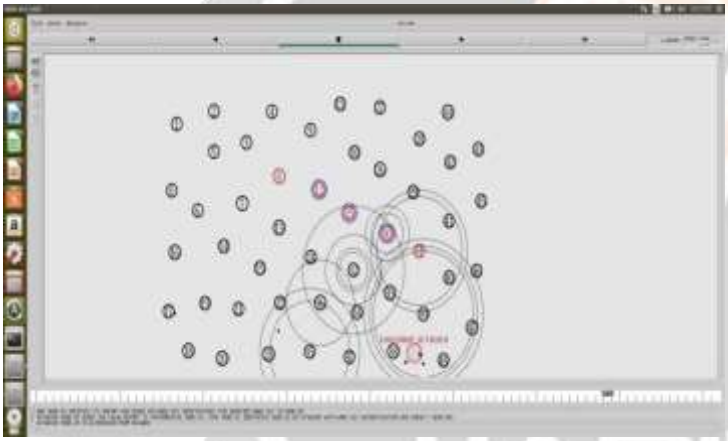


Fig 5:- After identifies the attacker in the network than the attacker node 49 is eliminted from the network

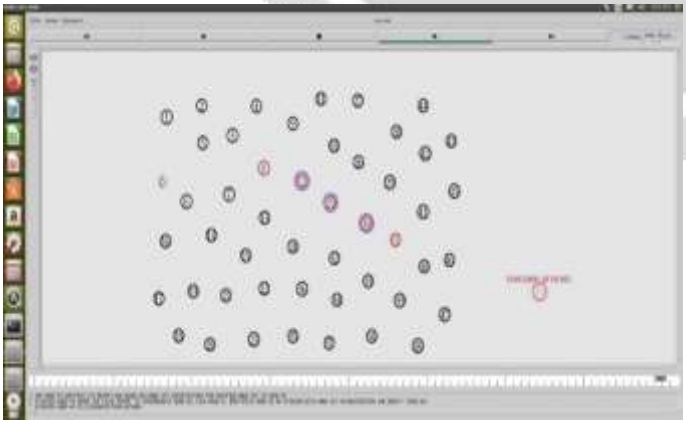


Fig 6:- After identifies the attacker in the network than the attacker node 49 is eliminted from th network

6.1 PERFORMANCE METRICS: THROUGHPUT:

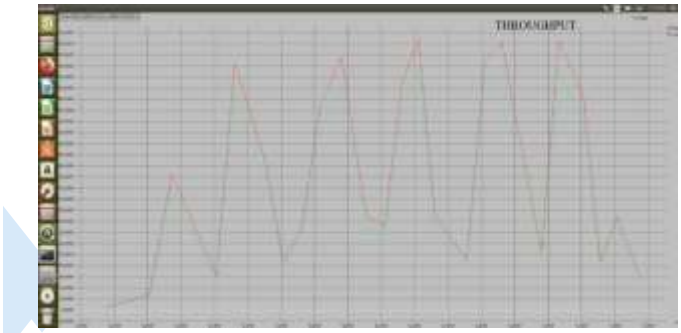


Fig 7 :-through put analysis

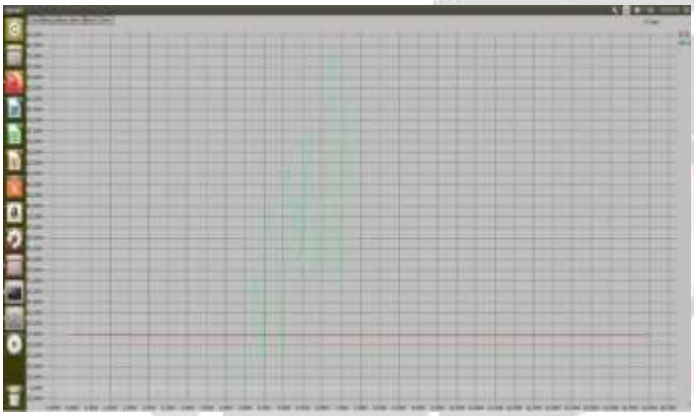


Fig 8:- End-to-End Delay:

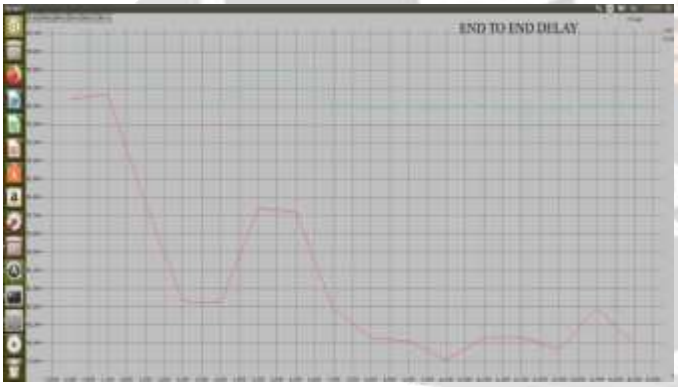


Fig 9:- End-to-End Delay:

7 . CONCLUSION:

One of the most important concerns in mobile ad hoc networks is security. I've emphasised several security requirements by comparing the performance of routing protocols for mobile ad hoc wireless networks, as well as a proposed method for securing transmission in these networks. The proposed security solution is one of various options for safeguarding data transmission in mobile ad-hoc networks. However, while reactive protocols performed well in high mobility scenarios, there is a clear need to implement more efficient techniques in mobile ad-hoc networks to address a variety of challenges other than security.

REFERENCES

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," in *Proc. IEEE Int. Ad. Comput. Conf.*, 2009, pp. 2112–2117.

[2] A. Chandra, "Ontology for manet security threats," in *Proc. 2nd Nat. Conf. Netw. Eng.*, 2005, pp. 171–

117.

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," *Int. J. Comput. Sci. Secur.*, 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 *Proc. 22nd Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process.*, 2014, pp. 428–431.

[5] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in *Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops*, 2004, pp. 698–703.

[6] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," RFC 3626, Oct. 2003, Doi: 10.17487/RFC3626.

[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 *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2007, vol. 2, pp. 249–256.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in *Proc. 8th Int. Symp. Wireless Commun. Syst.*, 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," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38–47, Feb. 2004.

[10] N. Garg and R. Mahapatra, "Manet security issues," *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, pp. 241–246, 2009.

[11] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, "An evaluation of protocols for uav science applications," NASA Technical Reports (NTRS), 2011 Earth Science Technology Forum (ESTF2011, Jun. 2011.

[12] A. R. McGee, U. Chandrashekhar, and S. H. Richman, "Using itu-t x. 805 for comprehensive network security assessment and planning," in *Proc. 11th Int. Telecommun. Netw. Strategy Planning Symp.*, 2004, pp. 273–278.

[13] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, 2002.

[14] F. Hong, L. Hong, and C. Fu, "Secure OLSR," in *Proc. 19th Int. Conf. Adv. Inf. Netw. Appl.*, 2005, vol. 1, pp. 713–718.

[15] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure, "Secure extension to the OLSR protocol," presented at the OLSR Interop Workshop, San Diego, CA, USA, 2004.

[16] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol.*, 2012, pp. 535–541.

[17] S. Maity and S. K. Ghosh, "Enforcement of access control policy for mobile ad hoc networks," in *Proc. 5th Int. Conf. Secur. Inf. Netw.*, 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 *Proc. 10th Int. Conf. Internet Technol. Secured Trans.*, 2015, pp. 391–398.

[19] S. Bhattacharya and T. Basar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in *Proc. Amer. Control Conf.*, 2010, pp. 818–823.

[20] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: A manet routing proto- col that can withstand black hole attack," in *Proc. Int. Conf. Com-put. Intell. Secur.*, 2009, vol. 2, 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 Netw.*, 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*, Jun. 1999, Doi: 10.17487/RFC2560.

[23] N. Doraswamy and D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Upper Saddle River, NJ, USA: Prentice Hall Professional, 2003.

[24] A. Ghosh, R. Talpade, M. Elaoud, and M. Bereschinsky, "Securing ad-hoc networks using IPSEC," in *Proc. IEEE Mil. Commun. Conf.*, 2005, pp. 2948–2953.

[25] K. N. Ali, M. Basheeruddin, S. K. Moinuddin, and R. Lakkars, "Manipsec-ipsec in mobile ad-hoc networks," in *3rd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, 2010, vol. 1, pp. 635–639.

[26] E. Rescorla, "Diffie-hellman key agreement method," *RFC 2631*, Jun. 1999, Doi: 10.17487/RFC2631.

[27] L. Harn, M. Mehta, and W.-J. Hsin, "Integrating diffie-hellman key exchange into the digital

signature algorithm (DSA)," *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 198–200, Mar. 2004.

[28] H. Krawczyk and P. Eronen, "Hmac-based extract-and-expand key derivation function (HKDF)," *RFC 5869*, May 2010, Doi: 10.17487/RFC5869.

[29] A. Adekunle and S. Woodhead, "An aead cryptographic frame- work and tinyaead construct for secure wsn communication," in *Proc. Wireless Adv.*, 2012, pp. 1–5.

[30] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numerische Mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[31] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623- dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Modeling Comput. Simul.*, vol. 8, no. 1, pp. 3–30, 1998.

[32] An open-source implementation of SUPERMAN is in develop- ment consisting of a Linux Kernel Module and Daemon. (2016). [Online]. Available: https://bitbucket.org/wj88/superman/