iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Literature Review on Existing Schemes on Basic Secure Routing Protocols in MANETs

A.VANI[1]
[1]*ECE Department, CBIT. Hyderabad.*

Abstract: Mobile Ad hoc Network (MANET) is assembled as a self-organized network with mobile nodes with a dynamic infrastructure. Designing of secure routing protocols is very difficult because of its characteristics. Moreover, protocols are designed with assumption of no malicious or selfish nodes in network. Hence, to design robust and secured routing protocols several effects made from researchers. In this paper, review on literature survey on basic secure routing protocols presented. The survey is categorized to Basic Routing Security Schemes, Trust-Based Routing Schemes, Incentive-base schemes, Schemes which employ detection and isolation mechanisms.
Keywords: MANET, Routing, Security, AODV, SEAD

I. INTRODUCTION

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Because of their security vulnerabilities these networks are very much exposed to attacks. According to different classification criteria, these attacks could be categorized in different ways. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication.

Additionally, attacks against MANETs can also be distinguished between two levels: attacks against the basic functionalities (e.g., multimedia access control at the MAC layer, routing at the network layer) and against security mechanisms. Attacks in the latter category are mainly cryptography related and notably against the key management mechanisms. The basic secured routing protocols used for MANETs are ARAN, ARIADNE, SAODV, SAR, SEAD and SRP. Research have shown that misbehaving nodes in a MANET can adversely affect the availability of services in the network[15] The existing schemes which attempt to mitigate against these miss behaviours use three main approaches:

II. BASIC ROUTING SECURITY SCHEMES

The routing schemes which fall in this category provide security services like authentication and integrity services which guard against modification and replaying of routing control messages, but they do not provide solutions for issues such as the dropping of packets by selfish or malicious nodes.

L. Venkatraman and D.P. Agrawal introduced an inter-router authentication scheme [1] for securing AODV [96] routing protocol against external attacks (such as impersonation attacks, replaying of routing of control messages and certain denial of service attacks). The scheme is based on the assumption that the nodes in the network mutually trust each other and it employs public key cryptography for providing the security services. The integrity of routing requests are ensured by the originating node hashing the messages and signing the resulted message digest. Recipients of a route request can check its authenticity and integrity by computing the hash of a message using the agreed upon hash function, compare the computed hash with that attached to the message and verifying the signature. Strong authentication" is provided for adjacent pair of nodes which transmit route replies. The strong authentication procedure is as follows: A node n_i sends a pre-reply plus a random challenge (challenge 1) to a neighbor it wishes to send a reply. The neighbor n_j which received the pre-reply generate a random challenge (challenge 2), encrypts challenge 1 with n_i's public key and sends the encrypted challenge along with challenge 2 to n_i. When n_i receives this message, it encrypts challenge 2 with n_j's public key and sends the route reply along with the encrypted value of challenge 2 to n_i. This procedure is designed for detecting nodes which attempt to impersonate other nodes.

P. Papa dimitrators and Z.J Haas presented secure routing protocol (SRP) [2]. SRP assumes the existence of a security association between a node initiating a route request query and the sought destination. The basic operation is as follows: A source node S initiates a route discovery by constructing and broadcasting a route request packet containing a source and destination address, a query sequence number, a random query identifier, a route record field (for accumulating the traversed intermediate nodes) and the message integrity codes (MIC) of the random query identifier, computed using HMAC and the secret key shared between the S and the destination. Intermediate nodes relay the route request packet so that one or more query packet(s) arrive(s) at the destination.

©IJRASET (UGC Approved Journal): All Rights are Reserved

When the route requests reach the destination D, D verifies that (a) the MIC is indeed that of the random query identifier, and (b) the sequence number is equal to or greater than the last known sequence number from S. If both (a) and (b) hold, D constructs a corresponding route reply packet containing the source, destination, the accumulated route in the route record field of the request query, the sequence number, the random query identifier and the computed MIC of the above. D then sends the route reply to S using the reverse path in the route record field. When S receives a route reply packet it validates the info it contains and verifies the computed MIC. If all is well, it uses the ascertained route to communicate with D.

Y.Hu, A. Perrig and D. Johnson proposed the Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [3]. SEAD is a source proactive protocol which is based on the design of DSDV . SEAD uses one-way hash chains for authenticating the hop count values in advertised routes and routing updates messages, SEAD allows authentication to be done using broadcast authentication mechanisms such as TESLA , or TIK which require the network nodes to have time synchronized clocks. Alternatively, SEAD allows message authentication codes to be used to authenticate the sender of routing update messages; however, this is based on the assumption that shared secret keys are established among each pair of nodes.

Zapata presented secure AODV (SAODV) [4]. SAODV uses two mechanisms to secure AODV: digital signatures to authenticate non-mutable fields of the routing control message and one-way hash chains (as in the case for SEAD, outlined above) to secure hop count information.

Y.Hu, A. Perrig and D. Johnson proposed a routing security scheme called Ariadne [5] which is based on the design of DSR [6]. Ariadne uses message authentication code for authenticating routing control messages, and it requires time synchronization hardware for synchronizing the release of the secret keys used for generating the message authentication codes.

Sanzgiri and Dahill presented ARAN [7]. ARAN uses digital signatures to secure the routing control messages. In ARAN route discovery phase, a source node S constructs a route discovery packet (RDP), signs it, attaches its certificate and broadcasts it to its neighbors. When a node A, which is a neighbor of S, receives the RDP message, if it has not previously seen this message, it verifies the signature using the attached certificate, signs the RDP message, attaches its certificate and broadcasts it to its neighbors. An intermediate node B which is a neighbor of A, on receiving the RDP message, it validates the signatures using the attached certificate. B then removes A's certified and signature, records B as its predecessor, signs the message and broadcasts it to its neighbors. The process continues in this manner until a RDP message arrives at the destination D. D selects the first RDP message it received, uses it to construct a reply (REP) packet and unicasts it to S using the reverse path. Each node on the reverse path back to S validates its predecessor signature using the attached certificate, removes the signature and the certificate (if the certificate does not belong to the destination node D), signs the packet, attaches its certificate and forwards the packet to the next-hop. Eventually, S should receive the REP with the route it seeks

III. TRUST-BASED ROUTING SCHEMES

The routing security schemes which fall in this group assign quantitative or qualitative trust values to the nodes in the network, based on observed behavior of the nodes in question. The trust values are then used as additional metrics for the routing protocols. In this review commence with one of the earlier protocols.

Yi et al proposed a scheme called security-aware ad hoc routing (SAR) [8]. In SAR, nodes are categorized based on their security level. A secret group key is associated with each security level and it is shared amongst nodes which are classified at the given security level. SAR incorporate security attributes as route discovery parameters, such that a node can specify its preference with regards to the security level required for participation in the routing process.

Yan, Zhang and Virtanen proposed a trust evaluation based security solution [9]. The application of this scheme to MANET routing is similar in principle to the design of SAR [8], in that the trust (or reputation) of a node is used as a routing metric when deciding the next hop of a packet.

Nekkanti and Lee presented a trust based adaptive on demand routing protocol [10]. The authors articulated that the most effective way of preventing certain routing attacks is to totally hide certain routing information from unauthorized nodes. In this regard, the main aim of their proposed scheme is to mask the routing path between a source and a destination from all other nodes. The scheme is based on AODV. It stipulates that one of three possible encryption levels be applied to a route request packets (RREQ). The

©IJRASET (UGC Approved Journal): All Rights are Reserved

encryption levels are high encryption which requires a 128-bit key, low encryption which needs a 32-bit key, and no encryption. The security level of a node and the security level of an application determine which encryption level is utilized. The general idea is that the more trustworthy a node is, the less need there is to hide routing information from this node during a route discovery operation. A summary of the route discovery operation is as follows: A source node S which desires a route to a destination D constructs a RREQ packet. The RREQ has a field where the application can set the security level it requires. The source then utilizes the public key of the destination node D to encrypt (with the appropriate security level) the source ID filed of the RREQ packet and broadcasts it to its neighbors. When an intermediate node receives a RREQ packet it has not previously seen, if it not the destination, it adds its node ID to the packet signs it then encrypts it using the public key of D and broadcasts it to its neighbor. Eventually an RREQ packet should get to D. on receiving an RREQ packet, D verifies the signatures, decrypts the encrypted fields and verifies that the nodes in the path has the minimum required trust level. Of these validation operations succeed, it constructs a route reply (RREP) packet and an own-id and encrypts the RREP and the own-id with the public keys of the nodes in the reverse path to S (in the order that the nodes should receive the RREP packet); then D signs the encrypted RREP and broadcasts it to its neighbors. When an intermediate node n_i receives the RREP it will attempt to decrypt it; if the decryption operation fails, n_i discards the packet; otherwise, it updates its routing table, the RREP should get to the source S which will verify the signature and decrypts the RREP to ascertain te route it seeks.

Boukerche et al proposed secure distributed anonymous routing [protocol (SDAR) [16]. The main objective of SDAR is to allow trustworthy intermediate nodes to participate in routing without compromising their anonymity. SDAR utilizes a trust management system which assigns trust values to nodes based on observed behavior of the nodes, along with recommendation from other nodes SDAR requires each node to construct two symmetric keys, and shares one with its neighbors which have high trust values and the other with its neighbors which have medium trust values. When a node S desires to discover a routing path to a destination D, S constructs a routing request packet (RREQ), part of which is un-encrypted and the other part encrypted. The un-encrypted part of the RREQ contains necessary routing information such as the trust level requirement of the message and a one-time public key TPK. The encrypted part of the RREQ packet contains the destination ID; symmetric key Ks generated by S and the private key TSK for the one-time public key TPK, plus other information. Part of the encrypted portion of the message is encrypted with the public key for the destination D and the other portion is encrypted with the symmetric key Ks. S then encrypts the entire packet with the shared key for the appropriate security level of the message and broadcasts it to its neighbors. When an intermediate node n_i receives the RREQ packet, it discards the message if it is not able to decrypt it. If n_i succeeds in decrypting the message, n_i adds its ID and a session key K_i then signs the portion it added and encrypts it with the one-time public TPK embedded in the un-encrypted portion of the RREQ packet; n_i then encrypts the entire message with the key (of the appropriate security) it shares with it neighbors and broadcasts the message. Eventually the message should get to D which decrypts the message with the appropriate keys. After verifying the signatures, D constructs a route reply (RREP) and encrypts it, first using the symmetric key Ks S attached, then encrypts it again using the session keys K_i's in the order that the corresponding intermediate node should receive the RREP packet. D then forwards the RREP to its neighbor. The neighbor which is the intended next-hop will decrypt its portion of the packet and forwards it to its neighbors (one of which will be able to partly decrypt it). The process continues until the RREP gets to the source node S which will be able to decrypt the entire packet and ascertain the route it seeks.

Li and Singhal proposed a secure routing scheme [12] which utilizes recommendation and trust evaluation to establish trust relationships between network entities. The scheme uses a distributed authentication model which operates as follow: each network node maintains a trust table which assigns a quantitative trust value to known network entities. If a node S desires to know the trust value of a node n_i and n_i is not in S trust table, S sends out a trust query message to ascertain n_i's trust value to all the trustworthy nodes in S trust table. When a node n_j receives the trust query message, if n_i is in its trust table, it sends the indicated trust value to S; otherwise it sends out a trust query message requesting the trust value to the n_i to all the trustworthy nodes in its trust table. The process continues recursively until eventually a node which has n_i in its trust table forwards the trust value to the node which requested the info, which will in turn eventually the response gets to S. S consequently uses the responses to compute a trust value for the node in question. This distributed authentication model is used to determine the trustworthiness of the network nodes. The end result being that nodes which are considered untrustworthy are excluded from routing paths.

IV. INCENTIVE-BASE SCHEMES

In this section we present a brief description of proposed schemes which attempt to stimulate cooperation among selfish nodes by providing incentives to the network nodes. Buttyaan and Hubaux proposed an incentive-based system for stimulating cooperation in MANET's [13]. The scheme requires each network node to have a tamper resistant hardware module, called security module. The

©IJRASET (UGC Approved Journal): All Rights are Reserved

security module maintains a counter, called nuglet counter, which decreases when a node sends a packet as originator, and increases when a node forwards a packet. The operation of the scheme is as follows: when a node S desires to send a packet to a destination D, if the number of intermediate nodes on the path from S to D is n, then S's nuglet counter must be greater than or equal to n in order for S to send the packet. If S has enough nuglets to send the packet, S decreases its nuglet counter by n after sending the packet. On the other hand, S increases its nuglet counter by one each time S forwards a packet on behalf of other nodes. The value of a nuglet counter must be positive; therefore, it is within a node's interest to forward packets on behalf of other nodes, and refrain from sending large number pf packets to distant destinations.

Zhong, Chen and Yang presented sprite: A simple, cheat-Proof, credit-Based System for MANETs [14]. Sprite provides incentive for MANET nodes to cooperate and report actions honestly. Sprite requires a centralized entity called a Credit Clearance Service (CSS) which determines the charge and credit involve in sending a message. The basic operation of sprite is as follows: when a node receives a message; the node keeps a receipt to the CCS the message it has received / forwarded by uploading its receipt. The CCS then uses the receipt to determine the change and credit involve in the transmission of the message.

V. SCHEMES WHICH EMPLOY DETECTION AND ISOLATION MECHANISMS

This section contains a brief description of schemes which utilizes detection and isolation techniques. In this the review starts an earlier proposal. Marti et al [15] proposed a scheme for mitigating against the presence of MANETs nodes that agree to forward packet but fail to do so. The scheme utilizes a \watchdog" for identifying misbehaving nodes and a \pathrater" for avoiding those nodes. Each node has its own watchdog and pathrater modules. Watchdog operation requires the nodes within a MANET to operate in promiscuous mode: meaning that a node n_i that is within the transmission range of a node n_j should be able to overhear communications to and from n_j even if those communications do not involve n_i. Watchdog is based on the assumption that if a packet was transmitted to node n_i for it to forward the packet to node n_j, and a neighbouring node to n_i does not hear the transmission going from n_i to n_j then it is likely that n_i is malicious and should therefore be assigned a lower rating . Pathrater is responsible of assigning ratings. The rating is assigned as follows: when a node n_i becomes known to the pathrater. N_i is assigned a \neutral" rating of 0.5. The ratings of nodes which are on actively used path are consequently incremented by 0.01 every 200ms; whereas, anode's rating is decremented by 0.05 when a link to the node is surmised to be non-functional. \Neutral" ratings are bounded with an upper bound of 0.8 and a lower bound of 0.0; but a node always assign a rating of 1.0 itself. rather than selecting a path to a given destination based on the number of hops in the path, the pathrater selects the path which has the highest average rating.

Buchegger and Le Boudec proposed a protocol called CONFIDANT [16] that aims to detect and isolate misbehaving nodes in MANETs. CONFIDANT uses a form of reputation systems [99] where the nodes within a MANET rate each other based on observed behaviors. Nodes that are deemed to be misbehaving are placed on black lists and are consequently isolated.

Awerbuch et al presented a routing security scheme [17] aimed at providing resilience to byzantine failure caused by individual or colluding MANET nodes. The scheme utilizes digital signatures for authentication at each hop, and it requires each node to maintain a weight list consisting of the reliability metric of the nodes within the network. The weight list is used in the route discovery phase to avoid faulty paths. When faults are detected in established paths, an adaptive probing technique is launched in an attempt to detect the faulty links. Faulty links are given decreased rating and are consequently avoided.

Just and Kranakis [18] and Kargl et al [19] proposed schemes for detecting selfish or malicious nodes in an ad hoc network. The schemes involve probing mechanisms which are similar in functionality to that of Awerbuch et al[6] above

Patwardhan and Lorga [20] presented a secure routing protocol called Sec AODV. Sec AODV is based on AODV but unlike the latter, it requires each node in the MANET to have a static IPv6 address. The scheme allows source and destination nodes to establish secure communication channel based on the concept of Statistically Unique and Cryptographically Verifiable (SUCV) identifiers [83] which ensures secure binding between an IPv6 address and a key, without requiring any trusted certificate authority (CA). SecAODv also provides IDS (Intrusion detection system) for monitoring the nodes' activities.

Performance parameter	ARAN	ARIADNE	SAODV	SAR	SEAD	SRP
Type	Reactive	Reactive	Reactive	Reactive	Proactive	Reactive
Encryption Algorithm	Asymmetric	symmetric	Asymmetric	Symmetric/ Asymmetric	symmetric	symmetric
MANET Protocol	AODV/DSR	DSR	AODV	AODV	DSDV	DSR/ZRP

©IJRASET (UGC Approved Journal): All Rights are Reserved

Function	Uses cryptographic certificates to secure the route discovery and maintenance mechanism.	Uses symmetric cryptography to secure the route discovery and maintenance mechanism.	Uses asymmetric cryptography to secure the route discovery and maintenance mechanism.	Uses explicit cooperation trust relationships to secure the route discovery mechanism	Uses one-way hash functions to secure topology discovery	Uses symmetric cryptography to secure the route discovery and maintenance mechanism
Synchronization	No	Yes	No	No	Yes	No
Central Trust Authority	CA Required	KDC Required	CA Required	CA/KDC Required	CA Required	CA Required
Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	No	No	Yes	No	No
Integrity	Yes	Yes	Yes	Yes	No	Yes
Non-repudiation	Yes	No	Yes	Yes	No	No
Anti-spoofing	Yes	Yes	Yes	Yes		Yes
DOS Attacks	No	Yes	No	No	Yes	Yes

Table .1: Comparison of Basic Secured Routing Protocols for MANETs.

VI. CONCLUSIONS

Literature survey is based on Basic Secured Routing Protocols and existing techniques to provide security against different attacks. From the above literature survey it is understood, most of the existing or available Basic Secured Routing protocols provide authentication, integrity and confidentiality security services. These are implemented or tested using cryptography and key management techniques. The solutions that relay on these techniques are seem promising but too expensive for resource constrained in MANET and increase the overhead and complexity.

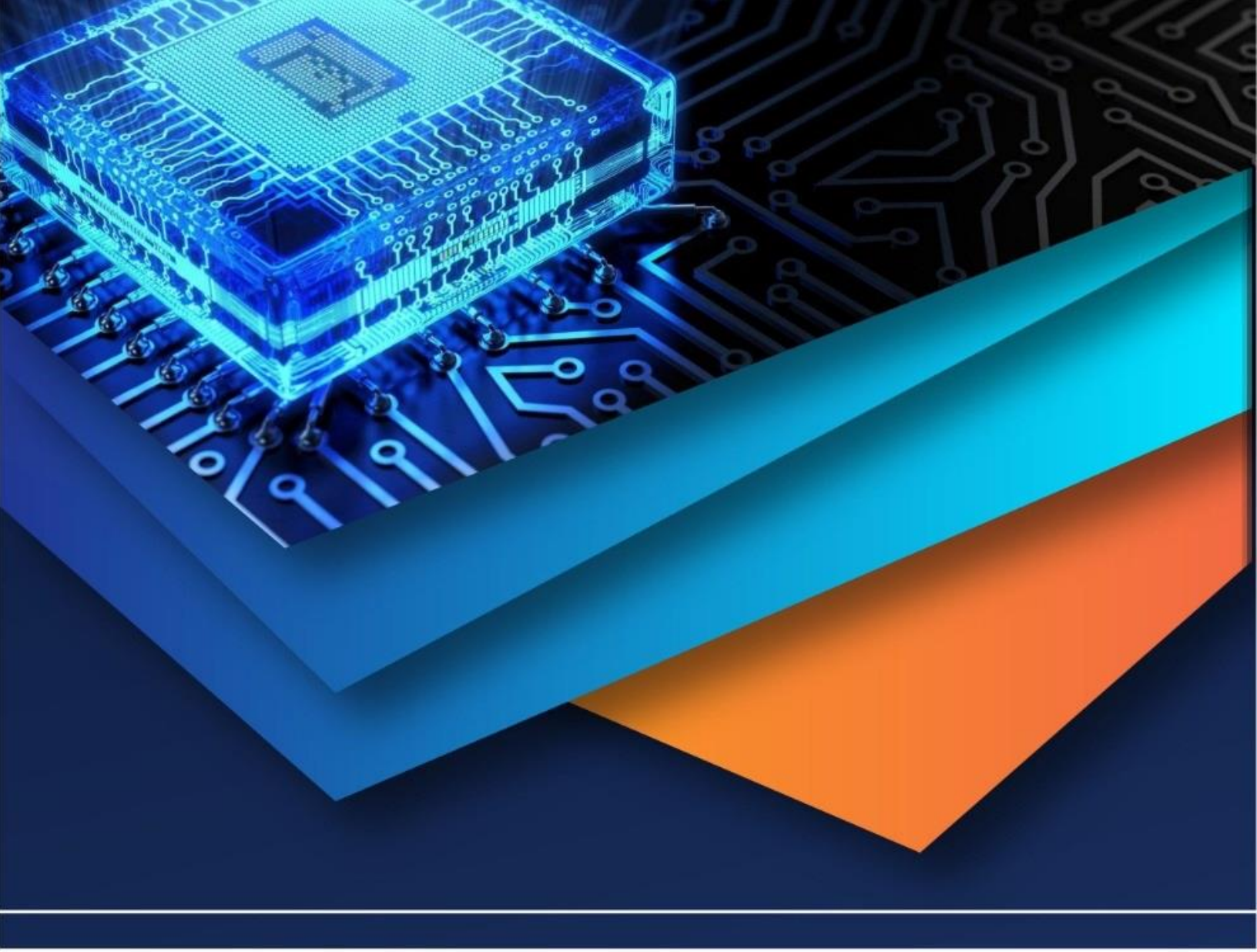
REFERENCES

[1] L. Venkatraman and D. P. Agrawal. An optimized inter-router authentication scheme for ad hoc networks. In Proceedings of the Wireless 2001, pages 129–146, July 2001.
[2] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002
[3] Y.C.Hu, A.Perrig,and D.B.Johnson.Ariadne:A Secure On-Demand Routing Protocol for Ad hoc Networks. In Proceedings of the Eight Annual International Conference on Mobile Computing and Networking(Mobicom),pages 12-
[4] M.Zapata and N.Asokan .Securing ad hoc routing protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe02), pages1-10 September 2002.
[5] Y. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in 8th ACM International Conference on Mobile Computing and Networking (MobiCom 2002), sssSeptember 2002.
[6] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (Mobicom 2002), pages 12-23, September 2002.
[7] K. Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E. M.Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP’02) 2002.
[8] S. Yi, P. Naldurg, and R. Kravets, “Security-aware ad hoc routing for wireless networks, Tech. Rep. UIUCDCS-R-2001-2241, August 2001.
[9] Z. Yan, P. Zhang and T. Virtanen, “Trust evaluation based security solution in ad hoc networks”, In the Proceedings of the Seventh Nordic Workshop on Secure IT Systems (NordSec 2003), 15-17 October 2003, Gjøvik, Norway.
[10] Nekkanti, R.K. and C.W. Lee, 2004. Trust based adaptive on demand ad hoc routing protocol. Proceedings of the 42nd Annual Southeast Regional Conference, Apr. 2-3, ACM Press, Huntsville, AL, USA, pp: 88-93. DOI: 10.1145/986537.98655
[11] Boukerche, A., K. El-Khatib, L. Xu and L. Korba, 2004. SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, Nov. 16-18, IEEE Xplore Press, pp: 618-624. DOI: 10.1109/LCN.2004.109 .
[12] H. Li and M. Singhal. A secure routing protocol for wireless ad hoc networks. In Proceeding of the 39th Hawaii International International Conference on Systems Science (HICSS-39 2006), pages 225–234, January 2006.
[13] S. Capkun, L. Buttya'n, and J.-P. Hubaux, “Sector: secure tracking of node encounters in multi-hop wireless networks," inProceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. Fairfax, Virginia: ACM, 2003, 986862 21-32.
[14] S. Zhong, J. Chen, and Y. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In Proceedings of IEEE INFOCOM, March 2003

©IJRASET (UGC Approved Journal): All Rights are Reserved

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Mobile Computing and Networking, pages 255–265, August 2000.
[16] S.Buchegger and J.Y.L.Boudec."Performance Analysis of the CONFIDANT Protocol.Cooperation of Nodes-Fairness"In Distributed Ad hoc Networking and Computing (MobiHoc), Pages 226-236.ACM Press, 2002.
[17] failures. In Proceedings of the ACM workshop on Wireless security (WiSE '02), pages 21–30, September 2002
[18] E. Kranakis, H. Singh, and J. Urrutia. Compass routing on geometric networks. In Proceedings of the 11th Canadian Conference on Computational Geometry, pages 51–54, August 1999.
[19] F. Kargl, A. Klenk, S. Schlott, and M. Weber. Advanced detection of selfish or malicious nodes in ad hoc networks. In Proceedings of the 1st European140 Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), pages 152–165, August 2004
[20] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T Karygiannis. Secure routing and intrusion detection in ad hoc . In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications , pages 191–199, March 2005

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)