iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A Secure Intrusion Detection System for MANETS in Receiver Collisions

D. Keerthi[1], Mr. CH. Samson[2]

M.Tech, Dept.of IT, Associate professor & Associate Head, Dept. of IT

Sreenidhi Institute of Science & Technology

Hyderabad, Telngana, India

***Abstract*—In this paper we mainly focusses on handling one of the drawbacks of Watchdog scheme to secure MANETs namely receiver collision. MANET is a collection of mobile nodes that forming a wired network. There are many challenges that are faced in Adhoc Network. The wireless nature of coomunication and lack of any security infrastructure raise several security problems. To handle the problem, a new intrusion detection system named Enhanced Adaptive Acknowledgement(EAACK) specially designed for Manets. The main focus has been laid on study of EAACK approach and its limitation.**

***Index Terms*— EAACK, AACK, MANET, Digital Signature, Receiver collision, WatchDog.**

I.INTRODUCTION

A mobile ad hoc network is a self-configuring dynamic network of mobile devices connected by wireless links with the set for a purpose. MANET is a collection of wireless mobile nodes forming a network without using any existing infrastructure The particular purpose may include, but not be limited to setting up a Adhoc network[1] for a military purpose like a combat regiment in the field. University school bus system with a number of school buses picking up students from different areas in city and in need of constant communication, and also in sensor networks where sensor data can be delivered to a central site for some specific purpose. One of the primary concerns related to adhoc networks is to provide a secure communication among mobile nodes in a hostile region. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture[3], a shared wireless medium and a highly dynamic topology. This last point is where the main problem for MANET security mentions: the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious node reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network. Similar to wired network and standard wireless networks, the first line of defending a MANET is constituted by intrusion detection systems like cryptography and authorization. However, the implementation of these type of mechanisms is not always possible due to the limitations that some nodes may present. On the other point, as it is well known, no matter how many intrusion prevention measures are inserted into a adhoc network, there are always some weak links that can attacked. In this case, the wireless and mobility aspects of MANET constitute two very vulnerable aspects for security. For this reason, it is necessary to implement a second line of defence through the implementation of intrusion detection and response to the mobile systems. These systems alert the network that an intrusion may take place and then take direct reactive and detective measures to protect the network. This is not always going to be successful in eliminating attacks against adhoc networks, but contributes to improve the security policies used to detect the possible threats and points of failure in the network. The main challenge is to construct intrusion detection and response solutions while preserving the desired network performance high-survivability network. For example, if an intrusion is detected in the early stage of a Distributed Denial of Service (DDoS) attack[7], a response can be put into place to minimize damages, gather evidence for prosecution and even launch counterattacks. So a new intrusion detection system is specially designed for MANETs to overcome the drawbacks of Watchdog scheme. In this paper mainly discussing about one of the drawbacks of existing system.

ISSN: 2321-9653

II.RELATED WORK AND BACKGROUND

Due to the limitation of most MANET routing protocol, nodes in MANETs assume that neighbour nodes always cooperate with other to relay data. This assumption leaves the attackers with the opportunities to achieve significant on the network with just limited compromised nodes. To address this drawback, IDS should be added to enhance the security level of mobile adhoc network[9][10]. If MANET can detect the attackers as soon as they enter in the network, we will be able to completely reject the potential damages caused by compromised nodes at the first time. In this Section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgement.

i)Watchdog:

The Watchdog theme is consisted of two elements, namely Watchdog and Pathrater. Watchdog detects malicious misbehaviour nodes by promiscuously being attentive to its next hop's transmission. If a watchdog node overhears that its next node fails to forward the packet from the source node among a particular amount of mentioned time, it will increase its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. Moreover, compared to another schemes, Watchdog is capable of police investigation malicious misbehaviour nodes instead of links. The watchdog theme fails to observe malicious misbehaviours with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) restricted transmission power; 4) false misbehaviour report; 5) collusion; and 6) partial dropping.

ii)TWOACK:

With respect to the six weaknesses of the above mentioned Watchdog scheme, several researches projected new approaches to unravel these problems. TWOACK detects misbehaving links by acknowledging each information packet transmitted over every three consecutive nodes on the trail from the supply to the destination. TWOACK is needed to figure on routing protocols like Dynamic Supply Routing. The operating method of TWOACK is shown in Fig. 1 : Node A primary forwards respected Packet to node B, and then, node B forwards that Packet 1 to node C. Once node C receives Packet 1, because it is two hops from node A, node C is duty-bound to come up with a TWOACK packet, that contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of packet one from node A to node C is fortunate. Otherwise, if this TWOACK packet is not received in an exceedingly predefined period, each nodes B and C area unreported malicious. Identical method applies to each three consecutive nodes on the remainder of the route.

III PROPOSED APPROACH

Our proposed approach is to solve the one of six weaknesses by TWOACK and AACK of Watchdog scheme, namely receiver collisions. In this section, In the receiver collision problem as illustrated in the Fig 1 the node A can only identify whether node B has sent the packet to node C or not, but node A cannot assure that node C has received it. If a collision occurs at node C when node B first forwards the packet, node A can only assume that node B has forwarded the packet and assumes that node C has successfully received it. Thus, B could skip rerouting and retransmitting the packet and evade detection.

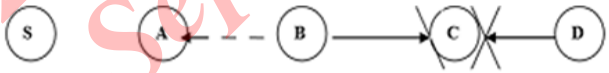


Fig 1 Receiver Collision.

In a typical type of receiver collisions, demonstrated in Fig 2, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding packet 2 to node C. In such case, node A overhears that node B has successfully, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node c.

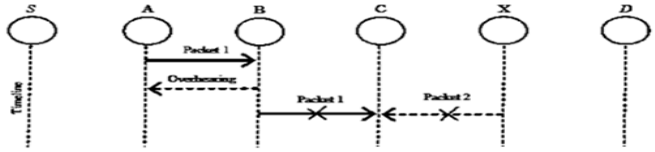


Fig 2 Receiver Collisions: both node B and node X are trying to send packets to node C at the same time

An ideal intrusion prevention model in MANET should first have a reliable, distributed, low-overhead, message collecting, and exchanging mechanism. The scheme should also adapt to changes in the network topology and tolerate message loss. Secondly, the model should be affordable for low computation power devices. Thirdly, the model should perform real-time protections since the routing topology may change very

quickly and the attack damage may also propagate relatively quickly. Finally, the model should not generate high false positives and negatives with respect to new routing attacks. Intrusion prevention is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". Intrusion detection system (IDS) is a practical approach to enhance the security of existing networks. Briefly, an intrusion detection system considers activity in a system or network in order to identify, to detect, and then to isolate current attacks. There are three main components of IDS namely i) Collection of data. ii) Analysis of collected data (Detection). iii) Response of an alert when a threat is detected.

For Mobile Ad hoc Networks, the general function of an IDS is detecting misbehaviours by observing the networks traffic in a MANET. Most of recent researches focused on providing preventive schemes to secure routing in MANETs.

In this we focus on analyzing the previous TWOACK and AACK method and intensively study the limitations of this system.

IV. DESIGN DESCRIPTION

The previous approach EAACK is designed to handle three of the six weaknesses of Watchdog Scheme, namely false misbehaviour, limited transmission power and receiver collision. In this section, here we discussing one of these three weaknesses namely Receiver Collisions in detail. In a typical type of receiver collisions, demonstrated in Fig. 3, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C;

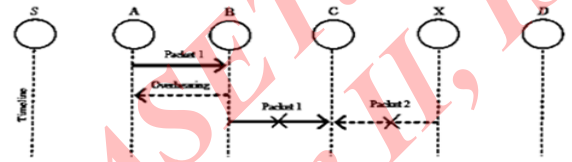


Fig.. Receiver Collisions: both node B and node X are trying to send packet 2 to node C at the time

meanwhile, node X is forwarding packet 2 to node C. In such this, node A overhears that node B has successfully, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet1 and Packet 2 at node C. Fig. 4 Receiver Collisions: both node B and node X are trying to send packet 2 to node C at the same time aas mentioned in previous sections, TWOACK and AACK tackle two of these three weaknesses, namely receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehaviour report attack. In this research work, our goal is to soolve the Enhanced Adaptive Acknowledgement (EAACK) scheme and analyze the limitation of this theme. As per previous edition the EAACK is an Enhanced intrusion detection system specially designed for MANETs, which solves not only receiver collision and limited transmission power, but also the false misbehaviour report Problem. EAACK was proposed and considered through implementation. In the previous work. The EAACK scheme was extended with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehaviours Report Authentication (MRA). In order to considered different types of packet in different themes, they included a two-bit packet header in EAACK. According to the Internet draft of DSR, there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets.

In the proposed scheme it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, both the source node and the destination node are not malicious nodes. Unless specified, all acknowledgement packets described in this paper are required to be digitally signed by its sender and verified by its receiver. We briefly describe the three major parts of EAACK.

A.EAACK:

This IDS is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce the network overhead when no network misbehaviour node is detected. In ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate mobile nodes along the route between node S and node D are cooperative and the node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ad1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak 1 P, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK Secure Acknowledgement mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

B. S-ACK: S-ACK theme is an implemented version of TWOACK scheme proposed by Liau at all. The rule is to let every three consecutive nodes work in a group to detect misbehaving malicious nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As demonstrated in Fig 3, in S-ACK mode, the every three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S. 1s adP 1 s adP 1 s akP 1 s akP. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report.

C. MRA:

The Misbehaviour Report Authentication (MRA) scheme is designed to solve the weaknesses of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehaviour report can be generated by malicious nodes to falsely report that innocent nodes as malicious. This attack can be considered to the entire network when the attackers break down sufficient nodes and thus cause a network environment. The core of MRA scheme is to authenticate the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another possible route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an another route to the destination node, we circumstance the misbehaviour reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

D. Digital Signature:

EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviours in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, [1] incorporated digital signature in their proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.

V. RESULTS

Our simulation is conducted within the Network Simulator(NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM.

In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, we ran every network scenario three times and calculated the average performance. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics [13].

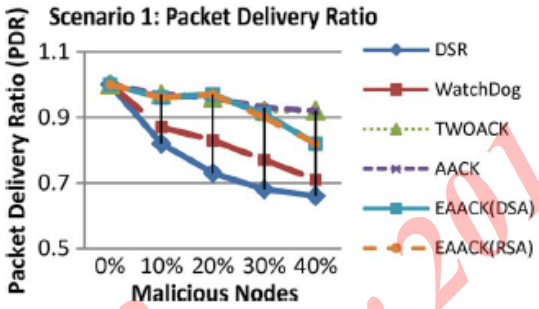
1)Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

ISSN: 2321-9653

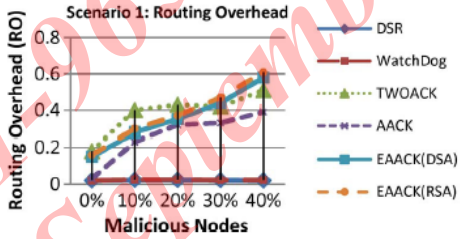
2)Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

During the simulation, the source route broadcasts an RREQ message to all the neighbours within its communication range. Upon receiving this RREQ message, each neighbour appends their addresses to the message and broadcasts this new message to their neighbours. If any node receives the same RREQ message more than once, it ignores it. Regarding the digital signature schemes, we adopted an open source library named Botan. This cryptography library is locally compiled with GCC 4.3. To compare performances between DSA and RSA schemes, we generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. The typical sizes of public- and private-key files are 654 and 509 B with a 1024-b DSA key, respectively. On the other hand, the sizes of public- and private-key files for 1024-b RSA are 272 and 916 B, respectively. The signature file sizes for DSA and RSA are 89 and 131 B, respectively. One of the most popular sensor nodes in the market is Tmote Sky [34]. This type of sensor is equipped with a TIMSP430F1611 8-MHz CPU and 1070 KB of memory space. We believe that this is enough for handling our simulation settings in terms of both computational power and memory space.

Scenario 1: Packet Delivery Ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	1	0.82	0.73	0.68	0.66
Watchdog	1	0.83	0.77	0.7	0.67
TWOACK	1	0.97	0.96	0.92	0.92
AACK	1	0.96	0.96	0.93	0.92
EAACK(DSA)	1	0.96	0.97	0.93	0.91
EAACK(RSA)	1	0.96	0.97	0.92	0.92
Scenario 1: Routing Overhead					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	0.02	0.023	0.023	0.022	0.02
Watchdog	0.02	0.025	0.025	0.023	0.023
TWOACK	0.18	0.4	0.43	0.42	0.51
AACK	0.03	0.23	0.32	0.33	0.39
EAACK(DSA)	0.15	0.28	0.35	0.44	0.58
EAACK(RSA)	0.16	0.3	0.37	0.47	0.61
Scenario 2: Packet Delivery Ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
DSR	1	0.82	0.73	0.68	0.66
Watchdog	1	0.83	0.75	0.69	0.68
TWOACK	1	0.93	0.84	0.82	0.79
AACK	1	0.93	0.85	0.82	0.8
EAACK(DSA)	1	0.95	0.92	0.87	0.79
EAACK(RSA)	1	0.95	0.92	0.86	0.79



Simulation results for scenario —PDR.



Simulation results for scenario —RO.

VI. CONCLUSIONS AND FUTURE SCOPE

Hence receiver collisions has been overcome by TWOACK and SACK in proposed system succesfully. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern implemented both DSA and RSA digital signature scheme in proposed approach. The goal was to find the most optimal solution for using digital signature in MANETs. Digital signature algorithms are used to provide authentication of data and validating the sender. Algorithms discussed include the signature algorithms RSA and DSA.

REFERENCES

[1] U. Sharmila Begam, Dr. G. Murugaboopathi A Recent Secure Intrusion Detection System for MANETs, Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, January 2013- here 1.

[2] EAACK - A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE Nan Kang and Tarek R. Sheltami, Member, IEEE.

[3] R. Akbani, T. Korkmaz and G.V.S Raju."Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127,pp. 659-666, Springer,2012 –here2.

[4] R.H. Akbani, S. Patel, D.C. Jinwala. "DoS Attacks in Mobile AdHoc Networks: A Survey", the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies(ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. –here2.

[5] T. Anantvalee and J. Wu. A Survey on Intrusion D etection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer, 2008.

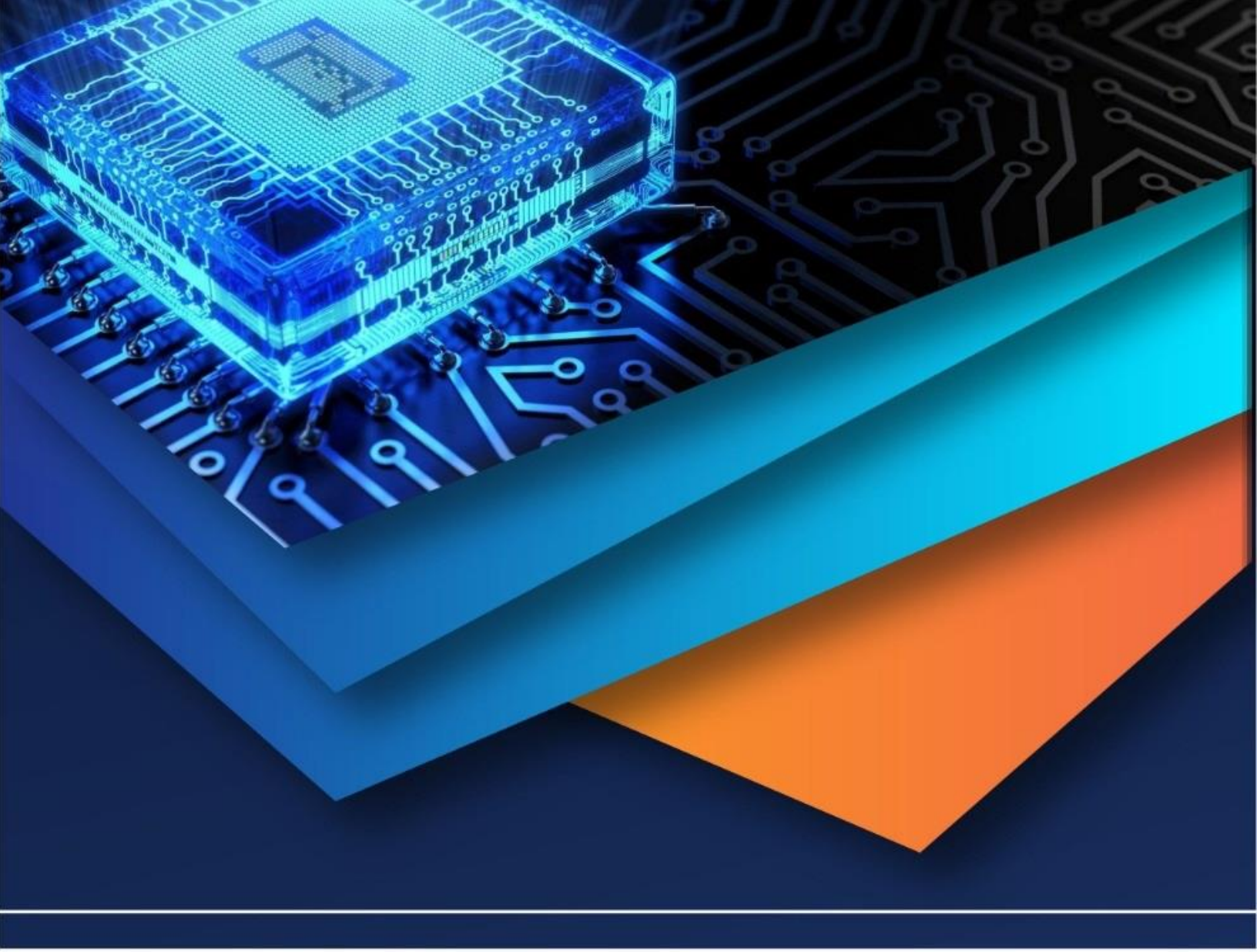
[6] L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[7] A. Singh, M. Maheshwari and N. Kumar. "Security and Trust Management in MANET", in Communications in Computer and Information Science, vol. 147, part 3, pp. 384-387. Springer, 2011–here 2

[8] B. Sun. Intrusion Detection in Mobile Ad hoc Networks. Doctoral Dissertation. Texas A&M University, 2004.

[9] K. Stanoevska - Slabeva and M. Heitmann. Impact of Mobile Ad- Hoc Networks on the Mobile Value System. 2nd Conference on m-Business, Vienna, June 2003.

[10] A. Tabes1h, L. G. Frechette, "A Low-Power Stand-Alone Adaptive Circuit for Harvesting Energy From a Piezoelectric Micropower Genera," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 840-849, March 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY