Journal of Advances in Science and Technology
Vol. 18, Issue No. 2, September–2021, ISSN 2230-9659

An Analysis the Auto-Configuration Address Protocol of Intrusion Prevention for Manets

Balendra Kumar Garg[1]*, Dr. Vijay Singh[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Associate Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - IoT are connected with each other and they operate in unprotected environments, it introduces more number of new constraints, issues and challenges that require security to be focused in a new way, which does not exist in the present computing systems. WSN & MANET are the two important technologies in the construction of IoT system as they participate in sensing, environmental monitoring, data acquisition, heterogeneous communication methods, data processing, etc. Attackers can use Sleep Deprivation (SD) to cause a disruption to service by sending an excessive number of control packets that appear legit. The MANET's self-configuration process was studied as the first step. Using the Manufacturer Serial Number (MSN) of a node to create & assign an IP address has been found to be the primary cause of the SD attack, so a novel IP address configuration approach has been developed.

Keywords - MANET, WSN, IP Address, Internet OfThings, Intrusion Prevention System, DOSAttack.

----------X----------

INTRODUCTION

This chapter deals with the overall picture of MANET automatic address configuration. It discusses the various approaches of address configuration and presents a novel approach, which protects the MANET from the Sleep Deprivation attack. A mobile ad hoc network (MANET) is an IP-based unplanned network of a collection of mobile and wireless nodes. A significant amount of research has been conducted on MANETs since the idea of mobile wireless devices working together was proposed in the 1990s. It is a self-governing network independent of any fixed infrastructure or centralized administration. The IETF created the Mobile Ad hoc Networks Working Group (IETF website 2014), (IETF website 2007) in 1997, with the aim of standardizing the routing protocols for MANETs. MANET can be divided into two categories namely, single-hop and multi-hop (Hashmi *et al*. 2008). Every node in a single-hop network speaks with each other directly over the same radio spectrum. In a multi-hop network, on either side, nodes rely on other intermediary nodes to deliver the data if the destination node is outside of their radio range. (Hashmi *et al*. 2008). These kinds of networks have more difficulties and drawbacks than a conventional network. The topology of a MANET is dynamic and it changes rapidly and in a random fashion. Besides, in a MANET the participating nodes are heterogeneous in type and the link capacity also varies from one link to another. Furthermore, frequent disconnections, transmission errors, network configuration and a lot of security issues may occur to degrade the performance of a MANET. Finally, because of limited resources of the nodes an ad hoc network is constituted by battery operated devices.

ROUTING ATTACKS IN IOT NETWORKS

The information is transmitted from the source node to the destination node in the IoT networks. The transmission amongst the source & destination based on the single-hop or multi-hop broadcast. The malicious nodes propagate their activities during this route discovery or route forwarding towards the destination. It creates several types of possible attacks in the routing of information. The malicious nodes send a large amount of false routing information to its neighbors that will capture the data from its neighbor nodes. The RPL is a proactive routing protocol and its structure is based on the DODAG. This DODAG construction is based on the Objective Function (OF) like Hop Count (HC), ETX (Expected Transmission Count) and Energy. These objective functions are used to calculate the rank value of each node.

The rank value determines the position of the node in the RPL DODAG. Also, the rank is responsible to construct and maintenance of the RPL DODAG. Consequently, the attacker targets the rank property to disrupt the network performances. Hence, a malicious node can promote a false route with the fake routing information such as the lowest rank value, higher energy level, smallest hop count & latest version number. Therefore, other neighbor nodes update their routing table with the false routing information. Normally, all the attacks are

targeted to reduce the topology performances, demand of resources and heavy network traffic.

- **Blackhole Attacks:** The Blackhole attacks occur in the route discovery phase. Each node is responsible to forward the data packets to the destination. However, the malicious nodes request the neighbor nodes with the false routing information and the legitimate nodes send the data packets through it. Therefore, the malicious nodes instead of forwarding the packets, it drops all the data packets. Also, the severity increases when the packets are modified before being forwarded. Low packet delivery ratio & false route announcements are the result of this attack.
- **Wormhole Attacks:** This kind of attack includes multiple malicious nodes. The initial attacker node in a wormhole assault builds a tunnel or path with the second compromised node. The first attacking node receives the packets and sends them to the second compromised node. A wormhole assault is when two attacking nodes work together to create a tunnel. The routing methods in wireless sensor networks are seriously threatened by this assault. Because this attack makes it more difficult to find any pathways.In RPL, this attacks create a tunnel between two RPL instances which have a separate DODAG in each RPL Instance.
- **Sybil Attacks:** In Sybil attacks, a node takes many identities that may not necessarily be lawful. It does not impersonate any node, but it only assumes the identity of another among several nodes and it is causing redundancies in the routing protocol. It degrades data integrity, security and resource utilization [Dha, 15]. Generally, Sybil attacks target the network to get confused or damaged.
- **Greyhole Attacks:** The Greyhole attacks are similar to Blackhole attacks which drops the data packets but transmiting the routing control packets. Hence, attackers selectively drop the data packets and try to participate into full communication. Greyhole malicious node participates into route discovery process and updates the source route cach/routing table as shortest path. Malicious nodes capture the incoming data packets but drop them randomly [Sha, 16]
- **Sinkhole Attacks:** To force other nearby nodes to choose the path through it, a hostile node promotes fake routing messages in sinkhole attacks. The rogue node is used as a conduit for legal nodes' data packets. The rogue node will change or update the routing information after receiving information. This attack behaves like selective forwarding and blackhole attacks. It affects the network performances in the RPL protocol by using fake rank value.
- **Selective Forwarding Attacks:** The aim of this attack is to degrade the performances of the networks. This type of attacker nodes selectively drop some packets and transmit remaining packets. It is similar to blackhole attacks. Hence, the malicious nodes modify or suppress packets which can reliably forward the remaining packets. Consequently, this attack affects the packet delivery ratio and produces the packet delay [Jyo, 16].
- **Hello Flood Attacks:** IoT has limitations of system resources like battery power, communication range and processing capability. Low processing and low power make such networks vulnerable to various types of network attacks. One of them is hello flood attack. An adversary node is not a legal node in the network, but it can flood hello request to any legitimate node and break the security of WSNs. The cryptographic solutions used for these types of attacks which suffer from heavy computational complexity [Sin, 10].
- **Neighbor Attacks:** In RPL, after the attack is triggered, the malicious node will replicate any DODAG Information Object (DIO) messages and broadcasts them again. The nodes which receive this type of messages may not be within range. Moreover, if a new neighbor node advertises a good rank then the nodes may request it as the preferred parent and changes the route [Le, 13b].
- **Local Repair Attacks:** In local repair attacks, the malicious node starts to broadcast local repair messages periodically. The other nodes upon receiving the local repair messages will need to recalculate the route which is related to the malicious nodes [Le, 13b]. This types of attacks impacts the packet delivery ratio, produce packet delay and packet drops during route topology operation.
- **DODAG Information Solicitation (DIS) Attacks:** A new node that wishes to join the RPL network sends a DIS message to neighboring nodes that might wind up being its preferred parents in order to obtain topological information. A DIS attack occurs when an attacking node sends its neighbors DIS messages, causing the neighbors' nodes to reset their DIO timers under the presumption that a new node is attempting to join the network. As a result, the new node receives DIS messages from its neighbors indicating that they are willing to admit it into the network. However, the rogue node keeps sending DIS signals, which finally causes neighboring nodes to run out of resources.
- **Version Number Attacks:** Version number is an element of each DODAG Information Object message and related to the network. The version number is monotonically

increased by the root each time the DODAG root decides to form a new version of the DODAG in order to revalidate the integrity and allow global repairs to occur [Dvi, 11]. An attacker node could then communicate the modified version number field to neighboring nodes in order to disrupt the network.

- **Rank Attacks:** In RPL protocol, the rank value determines that the position of each node in the network. The rank value of a node is used to select the parents and routes. A node's rank moves from highest to lowest in a downward & upward manner. In order to lure nearby nodes as a better parent route to the target, a malicious node fudges its rank value. RPL lacks a way to guard against changes to nodes' rank values [Air, 17b].This kind of attack will create un-optimized route, routing loops, decrease the packet delivery ratio and increase control overheads.

SCHEME DESCRIPTION

The Auto Configuration Protocol with Intrusion Prevention (ACPIP) system is thoroughly explained in this section. The four main components of ACPIP are MSN, IP COMPUTE, the allotment table, & MNA (Malicious Node Alert) message.

Many auto-configuration mechanisms have already been put out in the studies. Even if the majority of current algorithms presumptively consider MANET to be secure, incorrect IP address assignment for MANET nodes results in the aforementioned sorts of attacks. In this chapter, a protocol is developed that uses the maxim "Every node must be allocated a one and only one IP address" to dynamically assign an IP address to each new node that joins the network. First, we will discuss an autonomous ad hoc network that operates on its own; eventually, this will be expanded to include ad hoc networks that are a part of the IoT. The foundation of our suggested protocol is a condensed cryptographic hash function that inputs a device address (DA) & outputs a 16-bit result. A 48-bit Ethernet MAC address, a Bluetooth, UWB, or 64-bit Zigbee address, as well as any other distinctive identification of a node wishing to join the MANET, may be used as the input. Figure 1 depicts the suggested strategy.

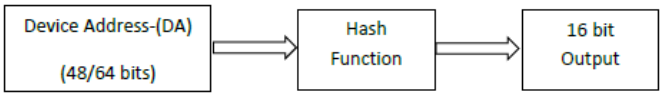

Figure 1: Block diagram of the proposed algorithm

SYSTEM MODEL

In this paradigm, a single node serves as the origin of an independent ad hoc network, & other nodes join the network one at a time. Nodes have complete freedom of movement & always free to join or exit the network. As a result, a dynamic topology will be generated, making it impossible to anticipate the network's size. The duration between the first node configuring itself with an IP address and all nodes leaving or turning off can be used to define the lifetime of the MANET.

Protocol Design Goals

The protocol must adhere to the following requirements in order to assign IP addresses:

a) A unique IP address should be assigned to each node in the MANET, ensuring that no more than one node at any given time has the same address. Additionally, a node should only receive one address for the duration of the MANET.

b) The protocol shall make sure that if a node departs the MANET and tries to re-join after some time (during the MANET's lifetime), the IP address provided to the node stays the same and should not be changed at any cost.

c) The protocol needs to be able to deal with network merging and partitioning scenarios. There is a chance that two or more nodes may share an IP address when two distinct MANETs converge. Such duplicate identities must be detectable by the protocol, and they must also be corrected.

d) The protocol must make sure that only approved nodes are set up & permitted access to the network resources.

The ACPIP Algorithm

The suggested algorithm for dynamic IP configuration is presented in this section. A MANET node's IP address can be determined using a device address (DA), such as an Ethernet MAC address, Bluetooth address, or any other analogous identification (hardware address of Zigbee or UWB protocol). The Auto Configuration Protocol with Intrusion Prevention (ACPIP) algorithm is the name of this system. Every node acts as a provider to a new node Nnew using the method here. As a result, all nodes have the ability to determine and issue IP addresses based on the new node Nnew's physical address, allowing Nnew to obtain an address solely from its neighbors. From the physical address provided by a new host, Nnew, each provider generates a distinct IP address for Nnew. Therefore, it is not necessary to broadcast a request message to search a server or for DAD.

PERFORMANCE EVALUATION

The experiments are conducted and analyzed the performance of the proposed idea using GLOMOSIM simulator. These experiments are focused at collecting the results of address

allocation Latency, Communication overhead and the number/type of messages exchanged by our protocol, at the same time preventing the attacks due to improper IP address assignments. This work is aimed to prevent two attacks namely (i) Sleep deprivation Attack and (ii) Sybil Attack by exclusively assigning IP address in a altered way. The following criteria are used to evaluate the ACPIP protocol:

- Random waypoint mobility model.
- Network area is 1000 m×1000 m.
- Nodes move with a maximum speed of 25 meters/second.
- The routing protocol used was AODV.
- Transmission range of the node is 100 m.
- Data link layer was IEEE 802.11 for all the nodes.
- The number of nodes in the network is 100
- Routing Protocol: AODV

The proposed technique for address assignment & intrusion detection is evaluated & contrasted with existing widely used protocols. The performance of ACPIP in comparison to other current schemes is shown in Table 1. The performance is measured using the following metrics:

Distributed process: Due to mobility, a small transmission range, and insufficient battery power, it is not feasible to designate a certain node as a configuration server in a MANET. As a result, the protocol ought to be shared throughout all of the MANET's nodes.

Complexity: It is attempted to make algorithms simpler by taking into account the constrained processing speed & memory capacity of mobile nodes.

Communication overhead: The answer consists of two parts. The first step is configuring the IP address, which solely calls for neighbor node communication. The MNA portion of the second component, which calls for broadcasting, is utilized to inform the nodes of the malicious node's entry.

Uniformity: The address range is evenly spread since the protocol is distributed across the nodes & IP addresses are created using cryptographic hash algorithms.

Table 1: Performance Comparison of ACPIP with other schemes

Metrics		MANET conf	Prophet	PrimeDHCP	PACMAN	SAAMAN	MMIP	ADIP	FAACP	ACPIP
Complexity		High	Low	Medium	Medium	High	Medium	Low	Medium	Low
Communication Overhead		High	Low	Medium	Medium	Medium	Low	Medium	Medium	Medium
Latency		High	Low	Low	High	High	Low	Medium	Low	Medium
Scalability		No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Uniqueness		Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Intrusion Prevention for Attacks	Sybil	No	No	No	No	No	No	No	No	Yes
	Sleep Deprivation	No	No	No	No	No	No	No	No	Yes

Latency: Since the protocol involves communication between neighbor nodes for address allocation, it creates only a shorter latency for address allocation.

Scalability: The scheme for address allocation allows every node as an address provider. Therefore, the number of nodes joining the network is not limited to the address space.

EXPERIMENT SETUP

To test the proposed ACPIP, a case study with various attack setups & analysis is made in this part. It shows the simulation results from these trials as well as some key findings from the attack investigation.

In the first experiment, a malicious RREQ flooding (MRF) attack is used to evaluate how well ACPIP defends against sleep deprivation attacks. Figure 3 displays the detection SR & FPR rate for the Sybil attack, whereas Figure 2 shows the success rate (SR) & false positive rate (FPR) of ACPIP by accounting for the number of nodes in the MANET with SD attack. Here, SR refers to the accuracy with which a network intrusion may be detected, along with the attack type & node that is launching it.

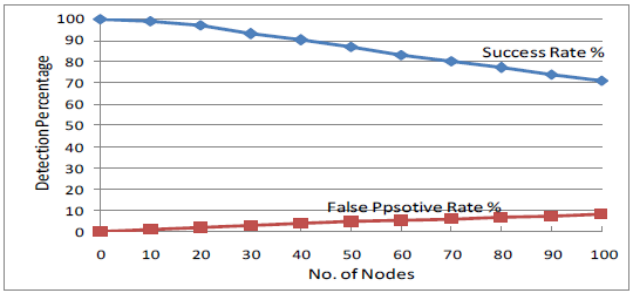

Figure 2: Success & False Positive rates of SD attack against the number of nodes

The False Positive Rate (FPR) means that a correctly behaving node has been wrongly identified and separated. The graph shows a better performance of ACPIP in terms of high SR and low FPR rates against the SD attack. Figure 3 shows the average address allocation latency in milliseconds when the nodes are moving at different speeds.

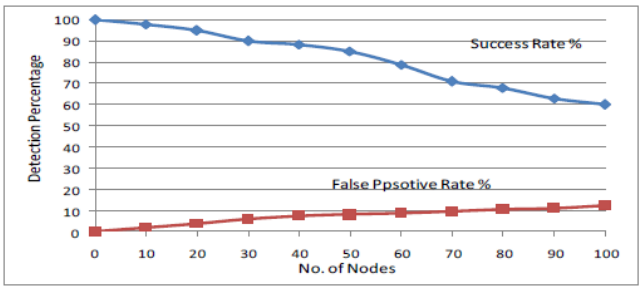

Figure 3: Success & False Positive rates of Sybil attack

Figure 4 shows the average protocol overhead in kilobytes when the nodes are moving at different speeds. Figure 5 shows the average message overhead and it is shown that ACPIO approach shows good results when comparing ACPIP with other existing protocols.

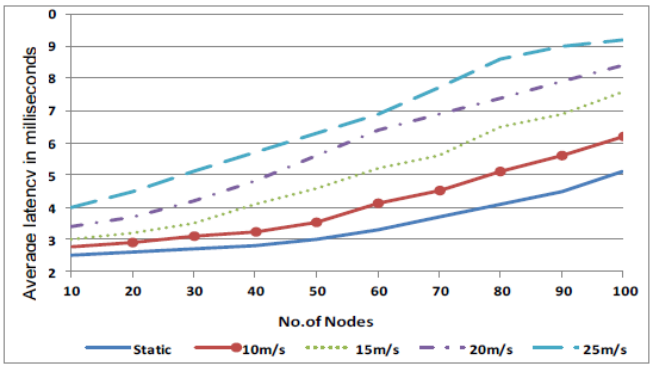

Figure 4: Average Address Allocation Latency in milliseconds

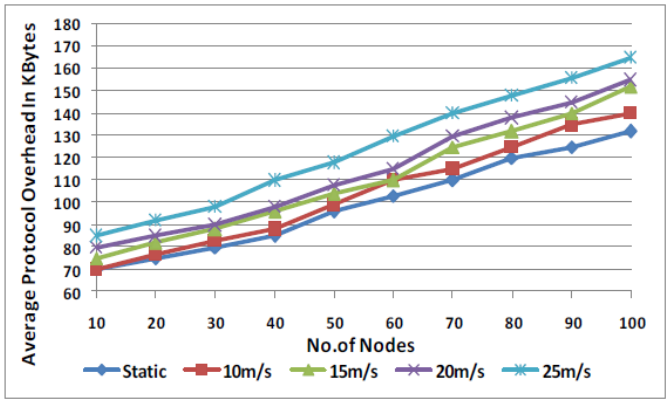

Figure 5: Average Protocol Overhead

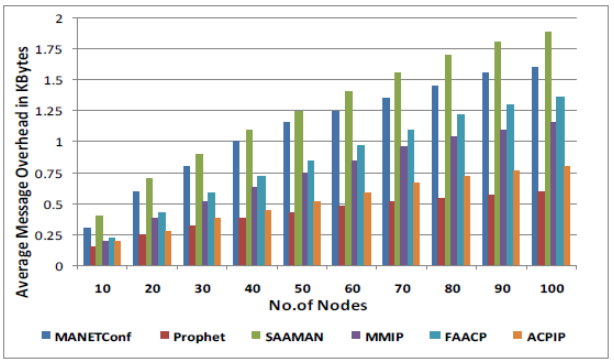

Figure 6: Average Message Overhead

CONCLUSION

This chapter has presented an innovative dynamic Intrusion Prevention System (IPS) by means of allocating a unique IP address for MANETs. In a MANET reassigning the unique address, when a node rejoins is a major challenge. IP address duplication after rejoining of a node in a MANET make it vulnerable for DoS attacks. The solution provides addresses, easily tolerate communication losses, splitting and reunion of MANET. The solution maps the MSN of a node with the allocated IP address. It guarantees that a node in a MANET will not be able to alter its IP address within the lifetime of the MANET, even if the MAC address of the node is changed. This removes the periodic message exchange between neighbors. In the algorithm, every host in the network acts as the address provider having the ability to assign IP addresses to new hosts. The signaling message excluding the MNA message need not be flooded over the MANET saving considerable bandwidth. No signaling message other than the MNA message is flooded over the MANET, which saves the considerable amount of bandwidth and battery power of nodes. The simulation experiments show that the proposed solution has reasonable latency, minimal communication overheads, uniqueness in providing IPv4 address and simultaneously preventing DoS attacks in a standalone MANET.

REFERENCES

1. Elijah, Olakunle, et al. "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges." *IEEE Internet of Things Journal* (2018).

2. Elijah, Olakunle, et al. "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges." IEEE Internet of Things Journal (2018).

3. Elsisi, M., Tran, M. Q., Mahmoud, K., Mansour, D. E. A., Lehtonen, M., &Darwish, M. M. (2021). Towards secured online monitoring for digitalized GIS against cyber-attacks based on IoT and machine learning. Ieee Access, 9, 78415-78427.

4. Farash, Mohammad Sabzinejad, et al. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment." *Ad Hoc Networks* 36 (2016): 152-176.
5. Farooq Muhammad Umar, Muhammad Waseem, AnjumKhairi, and SadiaMazhar, "A critical analysis on the security concerns of internet of things (IoT)", International Journal of Computer Applications, Vol. 111, Issue 7, 2015.
6. Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S., 2015, ‗A critical analysis on the security concerns of Internet of Things (IoT)', International Journal of Computer Applications, Vol.111, No.7.
7. Farras, Oriol, et al. "Optimal non-perfect uniform secret sharing schemes." *International Cryptology Conference*. Springer, Berlin, Heidelberg, 2014.
8. Fathallah, Karim, Mohamed Amine Abid and Nejib Ben Hadj-alouane, "Internet of things in the service of precision agriculture",the 1st Computer Science UTM PhD Symposium (CUPS'2017), Tunis, 2017.
9. Felipe da Rocha Henriques, Lovisolo, L. and Rubinstein, M.G., 2016, ‗DECA: distributed energy conservation algorithm for process reconstruction with bounded relative error in wireless sensor networks', EURASIP Journal on Wireless Communications and Networking, vol.1, pp.163.
10. Feng, Hailong, and Wenxiu Fu. "Study of recent development about privacy and security of the internet of things." *Web Information Systems and Mining (WISM), 2010 International Conference on*. Vol. 2. IEEE, 2010. 114
11. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016.
12. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.
13. Fette, I. and Melnikov, A, 2011, ‗The Web Socket Protocol,' RFC 6455 (Proposed Standard), Internet Engineering Task Force, [Online]. Available: http: //www.ietf.org/rfc/rfc6455.txt
14. Fielding, R. and Reschke, J, 2014, ‗Hypertext transfer protocol (HTTP/1.1): Message syntax and routing', RFC 7230 (Proposed Standard), Internet Engineering Task Force, [Online]. Available: http://www.ietf.org/rfc/rfc7230.txt
15. Fleisch, E., 2010, ‗What is the Internet of Things? An economic perspective', Economics, Management & Financial Markets, Vol.5, No.2.
16. Foschini, L., Taleb, T., Corradi, A. and Bottazzi, D., 2011, ‗M2M-based metropolitan platform for IMS-enabled road traffic management in IoT', IEEE Communications Magazine, Vol. 49, No. 11, pp. 50–57
17. G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, ``On the energy cost of communication and cryptography in wireless sensor networks,'' in *Proc. IEEE Int. Conf.Wireless Mobile Comput. Netw. Commun.*, Oct. 2008, pp. 580_585.
18. GaddourOlfa and AnisKoubaa, "RPL in a nutshell: A survey", Computer Networks, Vol. 56, Issue 14, 2012, pp. 3163-3178.
19. Gamundani Attlee M, "An impact review on internet of things attacks", In Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on IEEE, 2015, pp. 114-118.
20. Ghosh, U. and Datta, R., 2009, ‗ADIP: An improved authenticated dynamic IP configuration scheme for Mobile Ad Hoc Networks', International Journal of Ultra Wideband Communications and Systems, vol.1, No.2, pp.102-117.
21. Ghosh, U. and Datta, R., 2009, ‗MMIP: A new dynamic IP configuration scheme with MAC address mapping for Mobile Ad Hoc Networks', In Proceedings Fifteenth National Conference on Communications.

Corresponding Author

Balendra Kumar Garg*

Research Scholar, Shri Krishna University, Chhatarpur M.P.