DOI: 10.21917/ijct.2022.0392

A SERVICE PACKAGE IDENTIFIER BASED SECURITY VERIFICATION ALGORITHM FOR WIRELESS MOBILE AD-HOC NETWORK

R. Sabitha[1] and G. Kiruthiga[2]

[1]*Department of Electronics and Communication Engineering, Hindustan College of Engineering and Technology, India*
[2]*Department of Computer Science and Engineering, IES College of Engineering, India*

Abstract

In general, the biggest problem with a mobile ad-hoc network is the threat to its security. This is because the mobile ad-hoc network is dismantled after a certain period of time, which spends a lot of time calculating its stability and greatly wastes its security dimensions. Thus, the security features on these temporary networks need to be strengthened as they pose the most threats. In this paper, a security algorithm designed in SID mode is proposed to fix security vulnerabilities in the wireless mobile ad-hoc network module. Its main feature is that its security definitions are defined according to the number of Service Package Identification assigned to it. The definition of numbers based on its importance is to make a list of related devices in order and, accordingly, bring those devices into the security module. Its security features have been improved so that the security modules remain active as long as the network is active.

Keywords:

Service Package Identification, Ad-hoc Networks, MANET, Security, Stability

1. INTRODUCTION

The SIDs are designed as a unique name to distinguish multiple W-MANET networks in the region, while wireless devices such as phones and laptops provide networks to broadcast their SIDs and a list of names [1]. You can start a new network connection by selecting a name from the list. In addition to getting the name of the network, the Wi-Fi scan determines whether each network has enabled wireless security options. In most cases, the device identifies the protected network as a lock symbol next to the SID [2]. The most wireless devices add to a user connection and connection option that monitors various networks. In particular, networks with certain SIDs can automatically set up a device for users by storing that setting in their profile. In other words, once connected, the device will usually ask if you want to save the network or reconnect automatically in the future [3]. This means that you can set up the connection manually without access to the network i.e. It can connect to the network remotely so that when in range, the device knows how to log in). Most wireless routers offer the option to disable SID broadcasting as a way to enhance the security of the Wi-Fi network, as customers need to know both passwords, the SID and the network password [4]. However, the efficiency of this technique is low because it is very easy to disable the SID from the title of the data packets flowing through the column [5]. Since the SID broadcasts are disabled for networks, you have to manually create a profile with username and other connection parameters.

- If wireless security options are enabled on the network, anyone can connect to it by knowing only the SID.
- Having the same name on another nearby network using the default SID increases the potential for confusing wireless clients. When a Wi-Fi device finds two networks with the same name, it will automatically try to connect to any powerful radio signal it wants, which may be an unnecessary option. In the worst case, a person may be dropped from their own home network and re-connected to a page that lacks internal access security [6].
- The selected SID on a home network should contain only general information. Some names help thieves unnecessarily target others with certain homes and networks.
- An SID may contain publicly visible attack language or encrypted messages.

These are used by public W-MANET networks and all types of W-MANET access points, including your home W-MANET network. Router manufacturers often offer default SIDs, such as Linksys or Net gear, but you can change it to anything you want if you have control over the W-MANET network and have administrative access [7]. An SID can be up to 32 characters in length. They are case sensitive, so network name is an SID different from network name. Some special characters like spaces, underlines, periods and lines are also allowed. The wireless router or other W-MANET base station broadcasts its SID, allowing nearby devices to display a list of available networks with names that can be read by humans. If the network is an open network, anyone can connect to the SID [8]. However, if the network is protected with WPA2 or some other type of encryption, a password will be required before people can connect. We recommend against hosting an open W-MANET network [9].

Once you connect to a Wi-Fi network with a specific SID, your device will usually try to connect to SIDs with that name in the future [10]. Things are much more complicated if there are multiple Wi-Fi networks with the same SID. If they are in the same area, for example, two networks labeled Home - some devices will automatically try to connect to the network with a strong signal, and some will try to connect to the first network they see [11]. Of course, if the two W-MANET networks labeled Home have different passwords, your device can only successfully connect to one of them. So, if you use the same SID as your neighbor, you will both face some connection issues until one of you changes it [12].

You need to choose a unique SID, especially if you live near a lot of people — for example, in an apartment building. This will prevent connection issues. You should also not disclose personal information such as your name or address on the SID, as anyone nearby may see that information [13]. Remember, you are broadcasting that SID to everyone nearby. To change the SID on the network you control, you need to access your router settings, sign in with administrator credentials, and change the SID or Wi-Fi network name [14]. This usually includes accessing your router web interface and changing W-MANET settings. If your home is not connected to the W-MANET and you do not know what your

router SID is, you can generally access the router configuration page and find the password [15]. If you are not on a W-MANET network, you can often connect to your router via a wired Ethernet cable. If you are unable to connect to your router, you may find the default SID printed on the router. This will work if you or someone else with access to the router does not replace it [16]. If this does not work, you can reset your router by pressing and holding the small Reset button to reset your settings to default. See the manual for your specific model router for more information. If you do not have a manual, you can usually find them online with a simple web search [17].

Many wireless routers can create a W-MANET network with hidden SID. But, even if you hide your SID, the router still transmits traffic wirelessly. W-MANET networks with hidden SIDs do not appear in the list of W-MANET networks on PC or smart phone, but they can be detected by anyone with easy-to-use wireless traffic monitoring software [18]. Even worse, creating a hidden network can lead to connection issues and actually expose your W-MANET connection details. When you use a hidden network, your device should constantly broadcast its name and try to connect to find it [19]. W-MANET was never designed to work this way [20]. To protect your W-MANET network, set a strong password using WPA2 encryption. Do not create a hidden W-MANET network which is actually less secure.

2. LITERATURE REVIEW

Sathiamoorthy et al. [1] introduced a three-tier fuzzy cluster algorithm for Wireless Ad-hoc Networking. It is describing a way of connecting a wireless device that conducts a communication operation without being a central device. Each device / terminal connects data to the ad hoc network front for other terminals.

Jafar et al. [2] discussed Ant-based clustering algorithm for Mobile ad-hoc networks. It is required fewer configurations and can be used quickly, so they feel when they need a small, usually temporary, inexpensive, all wireless LAN together. If the equipment for an infrastructure system network fails, they are a temporary downtime.

Banerjee et al. [3] discussed some useful for temporary wireless networks or computer-to-computer wireless networks, Internet connection and other direct wireless networks without the need for a router. You can set up your own Wi-Fi network to connect two or more computers.

Sathiamoorthy et al. [4] discussed some energy and delay efficient MANET. The Mobile ad-hoc provides a cheaper way of direct customer-to-client communication, without the need for access points. In emergency medical environments, where cable is not an option while running, they are easy to configure and deliver in the best ways to communicate with nearby devices in time-sensitive environments.

Bokhari et al. [5] discussed the different algorithms in Ad-hoc networks. The Ad-hoc networks are often given a temporary or degrading nature. Without network access control, for example, ad hoc networks could be vulnerable to attack. While the number of devices on the ad hoc network is relatively small, the performance is better than most users are connected to a regular network.

Agarwal et al. [6] discussed the survey of clustering algorithms. On devices in infrastructure mode, devices on the network prior to SSID broadcasting cannot be disabled. If the attackers usually fall within the signal range, they will have difficulty locating and connecting the temporary device.

Jayaraman et al. [7] introduced a water flow model. The number of devices grows in the ad-temporary system, and as the network grows larger it becomes more difficult to manage. Devices cannot be used on the Internet unless one of these is connected to the Internet and shared with others. If web sharing is enabled, the client running this function will encounter massive performance issues, especially if there is more than one device.

Logeshwaran et al. [8] discussed about the various resource allocation methods for device-to-device communication. Here the different information provided and the communication mechanism between two unknown devices was discussed. These types of devices were created the data modification issues. The unknown device identification mechanism was introduced here and this will help to prevent the data modification issues from the unknown devices

3. PROPOSED METHOD

The proposed Service Package Identifier based security verification (SPISV) algorithm structure shown in the following Fig.1. All broadband routers support a group of systems for setting up a home Internet connection via a connected broadband modem. The specific names of these systems differ between router models as shown in the admin console.

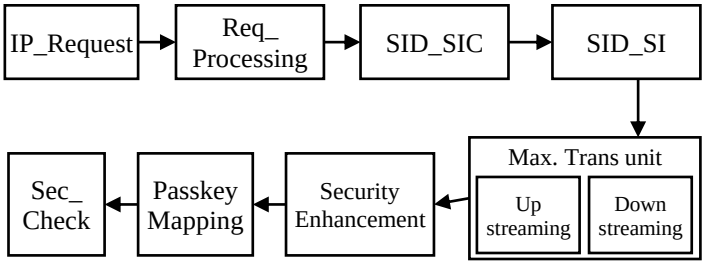

Fig.1. Proposed system architecture

- ***SID Secure Internet connection (SID_SIC):*** Home routers support all popular broadband internet service. Most routers provide a list of Internet connection types and require an administrator to select the one that best suits their network. Most types of connections listed in the router menu are named instead of the name of the Internet Service Protocol technology, rather than the name of the service provider. Typical choices for the type of Internet connection on a router include Dynamic IP (DHCP), Fixed IP, and PPPoE. PPTP and L2TP.
- ***SID Secure Information (SID_SI):*** Some Internet providers provide an account name and password for their subscribers, including Digital Subscriber Line (DSL). These systems must be logged in to the router console to support the modem.
- ***Maximum transmission unit (MTU):*** The maximum transmission unit system can have a very large number of bytes, network traffic network traffic. It is this value to multiple default numbers such as 1400, 1460, 1492 or 1500

to try to match values for a given type of internet connection. However, in some cases, the Internet provider network may require a different number. Attempting to visit websites using an inappropriate value can cause serious technical issues with the home network, including time constraints, so this number should be set as directed from the service provider.

Algorithm 1: Service Package Identifier based security verification (SPISV)

Step 1: Start

Step 2: Enter the IP-Request information

Step 3: Separate the process request as per the security guidelines

Step 4: Assign the user to secured internet connection

Step 5: If (USER = SIC)

Step 6: Then provide the data streaming to the user

Step 7: Then start transmission

Step 8: else

Step 9: Send the user for security check

Step 10: Update the user details in database

Step 11: end

One way to protect your network from unauthorized access is to hide the fact that you have a wireless network. By default, wireless network devices typically transmit a beacon signal, announcing its presence to the world and providing sensitive information needed to connect devices, including the SID.

The SID (Service Set Identifier) or network name of your wireless network, the devices you want to connect to it. If you do not want random wireless devices to connect to your network, you certainly do not want to announce your presence, and they need to include one of the key pieces of information that needs to be done.

$$SA(b) = 0.5\mu \int_{\sigma}^{0} \left|\nabla b(c)\right|^2 dc + \mu^{-1} \int_{\sigma}^{0} Q(b(c))\, dc \qquad (1)$$

where, SA(b) = Secured Connection Output; σ = Subnet of the given network; and $b(c)$ = Double Phase Security Check.

2	8	10	4	8	7
5	6	81	20	14	78
54	23	17	19	65	24
00	98	21	67	43	81
24	23	18	65	60	28
94	35	87	14	56	32

Initial Attributes

*

K	0	$-K$
K	0	$-K$
K	0	$-K$

Sec_Key

=

AK		

Final Attributes

Fig.2. Addition of different security attributes

By disabling the SID broadcast, or even the beacon signal, you can hide the presence of your wireless network or the SID itself, which is important for a device to connect to your network.

4. RESULTS AND DISCUSSION

The proposed Service Package Identifier based security verification (SPISV) was compared with the existing Residual energy based efficient communication (REBEC), Residual Distance based efficient communication (RDBEC), Dynamic selection of cluster head in WSN (DSCH) and Dolphin swarm inspired protocol (DSIP).

There are the following parameters are evaluating the security. That is the Security accuracy, input Security recognition, input Security rejection, Security precision, Security recall, and Security F1-Score. Before understand the quality rate of the parameters, will know about the following,

- ***Positive-T (TP)*** – It is the perfect predicted correct or above the calibration level.
- ***Negative-T (TN)*** – It is the negative prediction values below the calibration level.
- ***Positives-F (FP)*** – When the exact values are in calibration level and the predicted Entries are in same level
- ***Negative-F (FN)*** – When the exact values are in calibration level but the predicted Entries are in different level

4.1 MEASUREMENT OF INPUT SECURITY RECOGNITION

In general, input recognition is the process of effectively managing the excess information in a database. Due to its efficient use only the segmented data present in the Security database is used. Segmented data unnecessary data will not be allowed to enter. Thus, the blocking storage of the un-segmented data was restricted. Most storage space is handled efficiently if unwanted data is not stored.

Then, the un-segmented data blocking of a system is given by

$$\text{Input Security Recognition} = \sum_{a=1}^{h} I_j \qquad (2)$$

where, I_j is dented here the total number of input commands entered the system

The Table.1 presents the Measurement of Security recognition between existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.1. Measurement of input Security recognition

No. of Entries	Input Security recognition in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	67.69	71.01	76.58	70.72	96.44
200	67.36	69.51	75.99	68.85	95.43
300	66.02	68.4	75.01	68.02	95.27
400	64.88	68.02	73.8	67.11	94.31
500	63.83	67.01	72.66	66.19	94.74
600	63.12	66.08	71.55	64.86	93.54
700	61.82	65.08	70.85	63.78	93.38

4.2 MEASUREMENT INPUT SECURITY REJECTION

The input Security rejection management is the efficient handling of excess data provided. That is, how to quickly take action on information through artificial intelligence and implement it immediately. To the extent that it has its potential the results will be correct. Also, some data that was too much of the data given at the specified time may not even is processed. Thus, artificial intelligence management calculates how much data is left. The efficiency Measurement of this method refers to the fact that less data is not executed at that particular time.

Input Security Rejection = (*dropped instructions under the active production*/*non-block instructions arrivals* (3)

The Table.2 presents the Measurement of Security rejection between existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.2. Measurement of input Security rejection

No. of Entries	Input Security rejection in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	32.31	28.99	21.69	27.55	1.83
200	32.64	30.49	22.28	29.42	2.84
300	33.98	31.6	23.26	30.25	3
400	35.12	31.98	24.47	31.16	3.96
500	36.17	32.99	25.61	32.08	3.53
600	36.88	33.92	28.45	35.14	6.46
700	38.18	34.92	29.15	36.22	6.62

4.3 MEASUREMENT OF SECURITY ACCURACY

The Security accuracy is the parameter which describes the ratio between perfectly predicted Security input Securities from the given Entries to the total number of collected Security Entries. When the rate of Security accuracy is high then the given output Security sample getting high quality rate.

$$Accuracy = (TP+TN)/(TP+TN+FP+FN) \quad (4)$$

The Table.3 demonstrates the various measurement comparison of the Security accuracy values between the existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.3. Measurement of accuracy measurement

No. of Entries	Accuracy measurement in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	69.99	73.31	73.18	67.98	97.35
200	69.66	71.81	72.59	66.11	96.31
300	68.32	70.7	71.61	65.28	96.18
400	67.18	70.32	70.4	64.37	95.22
500	66.13	69.31	69.26	63.45	95.65
600	65.42	68.38	68.15	62.12	94.41
700	64.12	67.38	67.45	61.25	94.3

4.4 MEASUREMENT OF SECURITY PRECISION

Security precision measurement is the ratio between the positive true Entries and total true Entries. The total true Entries are calculated by the sum of positive true Entries and false positive Entries.

$$Precision = (TP)/(TP+FP) \quad (5)$$

The Table.4 demonstrates the various measurement comparison of the Security precision values between the existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.4. Measurement of precision measurement

No. of Entries	Precision measurement in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	68.73	81.05	80.74	76.42	96.61
200	67.1	79.31	79.16	75	95.32
300	66.62	76.97	76.96	73.74	94.31
400	65.33	76.16	75.33	71.75	93.42
500	63.22	73.87	74.19	69.28	93.05
600	61.73	71.94	71.99	67.84	92.01
700	59.92	70.21	70.84	66.12	91.24

4.5 MEASUREMENT OF SECURITY RECALL

Security recall measurement is the ratio between the positive true Entries and the sum of positive true Entries and false negative true Entries.

$$Recall = (TP)/(TP+FN) \quad (6)$$

The Table.5 demonstrates the various measurement comparison of the Security recall values between the existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.5. Measurement of recall rate

No. of Entries	Recall rate in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	78.62	76.95	80.58	75.41	96.61
200	77.13	74.98	78.16	73.21	96.62
300	76.33	73.85	77.75	72.41	95.42
400	74	72.66	76.15	71.74	94.94
500	72.99	72.27	73.83	70.31	93.51
600	72.35	70.75	72.58	69.22	92.35
700	71.69	70.51	69.85	68.74	91.58

4.6 MEASUREMENT OF SECURITY F1-SCORE

It is measured by the average sample values of Security precision and Security recall of the Entries.

$$F1\text{-}Score = (2*(Recall*Precision))/((Recall+Precision)) \quad (7)$$

The Table.6 demonstrates the various measurement comparison of the Security F1-Score values between the existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.6. Measurement of F1-Score

No. of Entries	F1-Score in (%)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	70.11	80.58	83.09	79.61	96.45
200	70.22	80.56	83.26	79.88	96.95
300	70.24	79.68	82.53	79.58	96.83
400	67.14	76.85	79.19	76.07	93.6
500	65.94	75.53	78.46	74.75	93.22
600	65.33	74.7	77.57	74.21	92.65
700	64.92	74.3	77.49	73.91	92.95

4.7 MEASUREMENT OF RECOGNITION TIME

The Measurement duration is nothing but the time taken to calculate the prediction of two different Securities.

Duration = (No. of Input Entries)/(Computation Speed) (8)

The Table.7 demonstrates the various measurement comparison of the Security recognition duration between the existing REBEC, RDBEC, GMBO, DSCH and proposed DSIP

Table.7. Measurement of recognition duration

No. of Entries	Recognition Duration in (ms)				
	REBEC	RDBEC	GMBO	DSCH	DSIP
100	13902	9020	11904	14103	2264
200	13125	8463	11499	13719	2098
300	12348	7906	11094	13335	1932
400	11571	7349	10689	12951	1766
500	10794	6792	10284	12567	1600
600	10017	6235	9879	12183	1434
700	9240	5678	9474	11799	1268

5. CONCLUSION

In general, the various security features in place deal with temporary mobile network features based on highly complex dynamic and unpredictable data systems. Various problems with this method made it unpredictable and further exacerbated its reliability shortcomings. This created major deficiencies in the protection of temporary natives. This system, which is currently being rolled out, is based on the Service Package Identifier based security verification method, so the value of the various services available on it continues to be found.

Data for the user is provided based on those calculations. The proposed SPISV model was compared with the existing REBEC, RDBEC, DSCH and DSIP. This provides the better results while compared with the existing models. Based on these results the temporary networking security features have been improved and its security vulnerabilities have been eliminated. This allows users to use it safely.

REFERENCES

[1] S. Kannan, G. Dhiman, and M. Gheisari, "Ubiquitous Vehicular Ad-Hoc Network Computing using Deep Neural Network with IoT-Based Bat Agents for Traffic Management", *Electronics*, Vol. 10, no. 7, pp. 785-796, 2021.

[2] M.E. Ahmed and H. Kim, "DDoS Attack Mitigation in Internet of Things Using Software Defined Networking", *Proceedings of International Conference on Big Data Computing Service and Applications*, pp. 6-9, 2017.

[3] S. Banerjee and S. Khuller, "A Clustering Scheme for Hierarchical Control in Multi-Hop Wireless Networks", *Proceedings of IEEE International Conference on Computer and Communications Societies*, pp. 102801037, 2001.

[4] L. Atzori and A. Iera, "The Internet of Things: A Survey", *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805, 2010.

[5] M.U. Bokhari, H.S.A. Hamatta and S.T. Siddigui, "A Review of Clustering Algorithms as Applied in MANETs", *International Journal Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 11, pp. 364-369, 2012.

[6] R. Agarwal and M. Motwani, "Survey of Clustering Algorithms for MANET", *International Journal on Computer Science and Engineering*, Vol. 1, No. 2, pp. 98-104, 2009.

[7] B. Gobinathan, M.A. Mukunthan, S. Surendran, and V.P. Sundramurthy, "A Novel Method to Solve Real Time Security Issues in Software Industry using Advanced Cryptographic Techniques", *Scientific Programming*, Vol. 2021, pp. 1-7, 2021.

[8] N. Arivazhagan, K. Somasundaram, D. Vijendra Babu and V. Prabhu Sundramurthy, "Cloud-Internet of Health Things (IOHT) Task Scheduling using Hybrid Moth Flame Optimization with Deep Neural Network Algorithm for E Healthcare Systems", *Scientific Programming*, Vol. 2022, pp. 1-8, 2022.

[9] P. Krishan, "A Study on Dynamic and Static Clustering based Routing Schemes for Wireless Sensor Networks", *International Journal of Modern Engineering Research*, Vol. 3, No. 2, pp. 1100-1104, 2013.

[10] M. Malik and Y. Singh, "Analysis of Leach Protocol in Wireless Sensor Networks", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, No. 2, pp. 178-184, 2013.

[11] T. Kothmayr, C. Schmitt, W. Hu, M. Br and G. Carle, "DTLS based Security and Two-Way Authentication for the Internet of Things", *Ad Hoc Networks*, Vol. 11, No. 8, pp. 2710-2723, 2013.

[12] M. Wazid, A.K. Das, V. Odelu and N. Kumar, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks", *IEEE Internet of Things*, Vol. 5, No. 1, pp. 269-282, 2017.

[13] G. Dhiman, K. Somasundaram and K. Sharma, "Nature Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking", *Mathematical Problems in Engineering*, Vol. 2021, pp. 1-21, 2021.

[14] S. Soni and B. Dey, "Dynamic Selection of Cluster Head in Cluster of Cluster Heads within the Cluster in Heterogeneous Wireless Sensor Network", *Proceedings of IEEE International Conference on Advanced Communications, Control and Computing Technologies*, pp. 877-881, 2014.

[15] N. Sabor, S. Sasaki, M. Abo Zahhad and S.M. Ahmed, "A Comprehensive Survey on Hierarchical-Based Routing Protocols for Mobile Wireless Sensor Networks: Review, Taxonomy, and Future Directions", *Wireless Communications and Mobile Computing*, Vol. 2017, pp. 1-19, 2017.

[16] X. Liu, "A Typical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review", *IEEE Sensors*, Vol. 15, No. 10, pp. 5372-5383, 2015.

[17] S. Anjali and M. Sharma, "Wireless Sensor Networks: Routing Protocols and Security Issues", *Proceedings of International Conference on Computer Communication Networking Technologies*, pp. 3-7, 2014.

[18] T. Bhatia, S. Kansal, S. Goel and A.K. Verma, "A Genetic Algorithm based Distance-Aware Routing Protocol for Wireless Sensor Networks", *Computer and Electrical Engineering*, Vol. 56, pp. 441-455, 2016.

[19] P. Sivakumar and M. Radhika, "Performance Analysis of LEACH-GA over LEACH and LEACH-C in WSN", *Procedia Computer Science*, Vol. 125, pp. 248-256, 2018.

[20] A. Peiravi, H.R. Mashhadi and S. Hamed Javadi, "An Optimal Energy-Efficient Clustering Method in Wireless Sensor Networks using Multi-Objective Genetic Algorithm", *International Journal of Communication Systems*, Vol. 26, No. 1, pp. 114-126, 2013.