I. J. Computer Network and Information Security, **2015, 6, 59-66**
Published Online May 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.06.07

ANM to Perceive and Thwart Denial of Service Attack in WLAN

Durairaj M
Assistant Professor, School of Computer Science, Engineering & Applications, Bharathidasan University, Trichy
durairajum@gmail.com

Persia A
Research Scholar, School of Computer Science, Engineering & Applications, Bharathidasan University, Trichy
persia_paradise@yahoo.co.in

Abstract—Wireless infrastructure network is vulnerable to Denial of Service (DoS) attack which makes the resources unavailable for its intended user. As an outcome of DoS attack, authenticated user is denied from accessing the network by spoofing legitimate client identity. Reduced protection in management frame led to MAC spoof DoS attack. Though 802.11w was developed to protect the management frame, the network is vulnerable to different DoS attacks and unable to prevent all types of DoS attacks. This motivated us to propose a mechanism to detect and prevent substantial number of DoS attacks. This paper proposes an algorithm called Alternative Numbering Mechanism (ANM) which prevents DoS attacks. The proposed solution is simulated in NS2 for experimentation. Packet delivery ratio, control overhead, normalized routing overhead, delay time, throughput and packet drop were measured for experimentation and to evaluate the performance of ANM. The experimental results of ANM demonstrate that the performance of ANM is encouraging and prevents nearly all types of DoS attacks.

Index Terms—Denial of Service Attack, MAC spoof, 802.11w, Wireless Local Area Infrastructure Network, ANM.

I. Introduction

In general networks are prone to security attacks predominantly wireless infrastructure network is more vulnerable to DoS attack. Easy and fast installation of wireless network which is due to technological advancements resulted in expansion of users. Security issues are increases proportionally as the user increases, where one of the major security issues witnessed is DoS attack. Security protocols such as 802.11i (JalilDesa et al, 2008), WEP (RadomirProdanovic et al, 2007), WPA (WiFi Protected Access) (Stanley Wong, 2003), 802.11 (John Bellardo et al, 2003), (Kemal Bichacs et al, (2009), 802.11b (Ferrari et al, (2008 802.1x and 802.1w) (ArashHabibiLashkari et al, 2009), (Nancy Cam Winget et al, (2003) are implemented over a WLAN (Wireless Local Area Network) to detect DoS attack. WEP (Wired Equivalent Privacy) uses RC4 algorithm which has many serious weaknesses. These security issues of network can only be controlled in some extent by introducing enhanced security measures. In 2004, IEEE 802.11i was ratified which is the most important phase of wireless security. Even though WEP has considerable security flaws, many companies are still using WEP because of the early espousal of wireless technologies (Brad Antoniewicz). The IEEE 802.11i introduced WPA and WPA2 to overcome the drawbacks of WEP. WPA/WPA2 encryption is stronger than WEP. WPA uses TKIP (Temporal Key Integrity Protocol) which can be hacked easily where WPA2 uses AES algorithm which is not easy to hack but requires more processing power than WPA. The AP and WiFi adapter must support WPA/WPA2 to apply these protocols. In order to achieve security, most hotspot uses WPA2.

Number of security encryption algorithms was deployed but still the weaknesses are there in the management frame. Management frame are not encrypted until 802.11w standard came into the work. 802.11w management frames are encrypted using AES-CCMP (Advanced Encryption Standard - Counter mode CBCMAC Protocol) algorithm. The AES-CCMP encryption algorithm could not prevent DoS attacks entirely. This algorithm prevents disassociation and de-authentication attacks which are sent after key establishment (2009). It is not possible for AES-CCMP algorithm to guard the frame which is sent proceeding of key establishment. The AES-CCMP is not widely spread over the world even though it prevents some of the DoS attacks. It is not popular across wireless community and not applied for security at present. A serious cause of DoS of attacks is the vulnerability of management frame and one of the popular mechanism to detect and prevent DoS attack is sequence number based detection system but it has some downsides (Kai Tao et al, 2008). As literatures say, there is no effective IEEE approved ways to solve the security hole in wireless infrastructure network.

This paper proposes an algorithm known as ANM which can be used to replace the sequence number field. Existing sequence number mechanism displays its incompetence to detect all type of spoofed frame. It is

difficult to apply sequence number mechanism into an existing AP (Access Point) or Station. Hackers can easily track sequence numbers and it is possible to launch DoS attack in easy spoofing. In some of the existing work from literatures, the experiments show that only first few spoofed frame are detected and the next consecutive frames go undetected whereas in (Anjum et al, 2005),first few frames will be successful. In (Cardenas), RARP (Reverse Address Resolution Protocol) request is used to detect spoofing but it is found to be unsuccessful when a hacker spoofs with IP address. It also leads to a number of false positive. In (Li et al, 2007), RARP request could detect spoofing but could not prevent the spoof based attack. This mechanism is not providing complete protection though the detection of first few frames is successful (Bansan et al, 2008), (Guo, F et al, 2006),

In this paper, Section II presents the background review and related work to understand the paper. Section III describes the possible attacks in WLAN. Section IV explains the architecture of the proposed technique and experimentations. Section V explains the ANM algorithm, which is to prevent the DoS attacks in an infrastructure network. Section VI describes the ANM and hybridization of ThreVANM in start frame and logoff frame attack. Section VII gives the experimental evaluation of proposed algorithms. Section VIII discusses the results and discussion of ANM and ThreVANM. Finally, Section IX concludes the paper.

II. Related Work

Fanglu Guo et. al, (2006), proposed an algorithm to detect spoofing by leveraging the sequence number field in the link-layer header of IEEE 802.11 frames and demonstrated how it can detect various spoofing without modifying the APs or wireless stations. This sequence number detection technique could not detect the entire spoofed frame. This algorithm detects first few spoofed frame whereas the succeeding frames go undetected. It uses RARP request to detect spoofing. In this work, MAC spoof detection is achieved when two IP addresses retrieved for a single MAC address.

Cardenas et. al., proposed a mechanism which detects the attack based on RARP request. If two IP address could be retrieved for single MAC address, it is considered as a spoofed frame. This solution is not applicable when a hacker spoofs IP address as well.

Yong Sheng et. al. (2008), proposes Gaussian Mixture Modeling (GMM) for Received Signal Strength (RSS) profiling to detect spoofing attacks using Multiple Air Monitors (AMs) which sniffs wireless traffic passively without the cooperation of Access Point (APs) and clients. In this method, accurate detection of MAC spoof is obtained using a GMM mechanism.

Tenatat Saelim, et. al.(2011), provides a MAC spoofing detection algorithm in IEEE 802.11 networks. To differentiate an attacker station from a genuine station, the proposed algorithm utilizes Physical Layer Convergence Protocol (PLCP) header of IEEE 802.11 frames. Experimental results provide a cent percentage of MAC spoofing DoS detection when two monitoring stations are located at an appropriate location.

III. Denial of Service Attack

The Denial of Service attack is an attempt to make computer resources unavailable to its legitimate users. Intruders can easily access the network by pretending themselves as authenticated users. Numbers of studies have been taken to avoid DoS attacks and different security protocols were also proposed. These protocols provide specific solutions to avoid DoS attacks, but none of them demonstrates cent percentage secured.

Security flaws presented in existing preventing mechanisms motivates the researchers to shape an efficient mechanism to protect the infrastructure network from MAC spoof DoS attacks. We propose Computerized Monitoring System (CMS) which combines Threshold Value (ThreV) (Durairaj et al, 2014), Alternative Numbering Mechanism (ANM) and Traffic Pattern Filtering with Letter Envelop Protocol (TPatLetEn). This paper only explains effects of ANM and hybridization of ThreV and ANM in DoS attacks. The future direction of this work is to combine these three algorithms and to develop more effective security system for network. In this paper, we proposed a solution which uses two tables such as Basic Identity Check (BIC) and Intruder Table (InT). To evaluate the performance of proposed algorithm, experimental tests with four different types of attacks were performed and six parameters were measured on attacks. Types of attacks engaged for the experimental study are:

- ✓ Start frame attack over AP
- ✓ Start frame attack over Client
- ✓ Logoff frame attack over AP
- ✓ Logoff frame attack over Client

To evaluate the effectiveness of the proposed algorithm, the following six parameters were measured.

- ✓ Packet delivery ratio
- ✓ Control overhead
- ✓ Normalized routing overhead
- ✓ Packet drop
- ✓ Delay time
- ✓ Throughput

IV. Proposed Solution To Detect And Prevent Attack

In this work, sequence number field is replaced with ANM. Weakness of the sequence number techniques leads us to propose ANM. Random guesses of sequence number is possible and attacks can easily be launched. ANM comprises of alternative odd decimal numbers which are 1.3, 1.5, 1.7....n. In ANM mechanism, the hackers cannot easily assume the exact alternative numbers presents in the header field. It is difficult for an

intruder to assume the apt ANM to make MAC spoof attack. If hacker somehow reaches out the exact ANM of client/AP, then responsibility will be redirected to TPatLetEn. In our previous paper, we proposed ThreV algorithm. This algorithm takes over the control when the source sends the packet to the destination and it checks in BIC and InT respectively. If the ThreV algorithm detects the hacker, it prevents the hacker to further entry into the network. If the packet is suspicious but unerring, the requested packet will be redirected to ANM to avoid the false positive. This mechanism gives effective result in detecting MAC spoof.

A. Alternative Numbering Mechanism (ANM)

Alternative numbering mechanism is used instead of sequence number field. The drawbacks presented in sequence number techniques leads to propose ANM. Random guesses of sequence number is possible and attacks can be launched in a simple manner. ANM comprises of alternative odd decimal number which is 1.3, 1.5, 1.7....n. Maintaining ANM, hackers cannot assume the exact alternative number which presents in the header field. It is difficult for an intruder to assume the apt ANM to make MAC spoof attack. If hacker finds out the exact ANM of client/AP, it should be redirected to TPatLetEn.

B. Architectural Framework of ANM

The requested packet's identity is checked in InT when Access point (AP) receives request from client. If the MAC address is presented, it rejects the request. Otherwise, it checks in BIC where the every LAN user's MAC addresses are presented. The request is accepted when the MAC address is presented in BIC table. After checking in BIC, ANM takes over the control of packet and checks the sequence number field.

ANM is used in this research instead of sequence number field. Default ANM is taken as 'i' and then it calculates current ANM (C_{ANM}). The C_{ANM} is calculated by adding 0.2 with D_{ANM}. If the obtained C_{ANM} is equal to the odd decimal number and the difference between C_{ANM} and P_{ANM} is 0.2 then it process the request. Otherwise, it is considered as spoofed frame and stores the hackers MAC addresses into InT. The proposed architectural frame work of ANM is as shown in Fig 1.

V. Detecting And Preventing DoS Attacks Using ANM

ANM is a mechanism which perceives and thwarts DoS attack in wireless infrastructure networks. This section explains the Start frame and Logoff frame attack and how these attacks can be minimized using ANM technique.

A. ANM in Start Frame Attack

Once client sends start frame request to AP, MAC address of client will be checked in InT whether the MAC address of the client presents in InT or not. If it presents, the request will be rejected, otherwise the user's identity will be checked in BIC table which contains all the WLAN users MAC addresses. It rejects the request when the MAC address is not presented. If the clients MAC address is presents in BIC, it will be redirected to ANM detection techniques. ANM of current packet is calculated after it gets request.

$$C_{ANM} = i + 0.2$$

Hence, D_{ANM} = i. where 'i' initialized as 1.1. When C_{ANM} = odd_no&& diff $_{ANM}$(C_{ANM} - P_{ANM}) gives 0.2, the system accepts start frame request and communication starts between client and AP otherwise this request is considered as a spoofed frame. Our proposed technique detects the original MAC address of the hacker and stores it in InT.

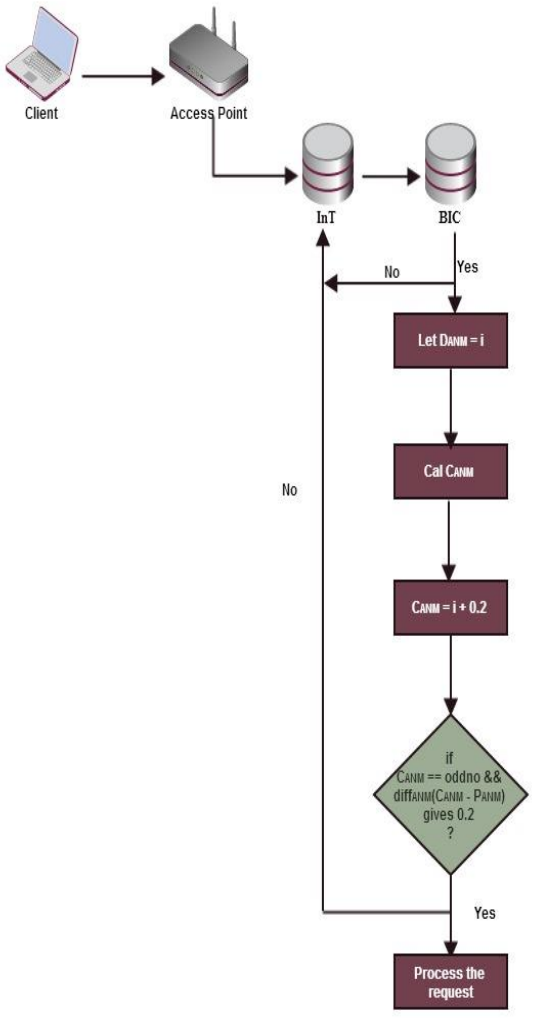

Fig 1. Architectural framework of the proposed ANM

The same process is followed while AP and Client are communicating with each other, if AP gets a start frame request from the existing users who is already in communication with AP and hackers can be identified easily by the ANM technique without affects the communication of AP and Client.

ANM - Algorithm for Start frame Attack
Step 1: Initialize i = 1.1
Step 2: Let D_{ANM} = i
Step 3: Calculate C_{ANM}
Step 4: C_{ANM} = i + 0.2
Step 5: if C_{ANM} == odd_no&&$diff_{ANM}$ (C_{ANM} - P_{ANM}) gives 0.2
Step 6: Process the request
Step 7: else
Step 8: Request rejected and store in InT

Algorithm 1: ANM for start frame attack over AP and Client

B. ANM in Logoff Frame Attack

During the communication period, when AP receives logoff request from client, it checks in InT. If the MAC address is not presented in InT, it will be redirected to BIC unless the request is rejected. After BIC checks the user identity, it will process this request to ANM. The proposed technique computes the alternative number of frame. If it gets alternative odd decimal number and the difference between alternation number of current frame and previous frame gives 0.2, the logoff request will be processed and the logoff continue message will be send back to the client by AP else the requested packet will be rejected and store it in InT.

The logoff algorithm describes that alternative number to current frame is calculated by adding i and 0.2, if current frame alternative number is odd decimal and the difference between the alternative number of previous frame and current frame gives 0.2, the request is treated as a legitimate one else the request is rejected and store the hackers original MAC address in InT.

VI. Detecting And Preventing DoS Attack Using Hybridization of ThreV and ANM

After AP receives request from client, the requested packet's identity is checked in InT. If the MAC address is presented, it rejects the request. Otherwise, it checks in BIC where the every LAN user's MAC addresses are presented. The request is accepted when the MAC address is presented in BIC table. After that, ThreV takes control over the requested packet. If AP receives single request within α, it is considered as a spoofed frame. If the transmitted packet is greater than one within α, it is taken as an anomalous packet and rejects the requested packet and stores it in InT. In some cases, there is a chance of occurring that the transmitted packet is one within α, it will be redirected to ANM for better prevention of MAC spoof DoS attack. In ANM, default ANM is taken as i then it calculates current ANM (C_{ANM}). C_{ANM} can be calculated by adding of 0.2 with D_{ANM}. If the obtained C_{ANM} is equal to the odd decimal number and the difference between C_{ANM} and P_{ANM} gives 0.2, the request will be accepted and redirect it to next prevention mechanism TPatLetEn for effective prevention of DoS attacks. In another case, if ANM is not a odd decimal number or the difference between C_{ANM} and P_{ANM} does not gives 0.2, the request will be rejected and stores the MAC address in InT.

A. ThreVANM in Start Frame Attack

The Algorithm-2 combines ThreV and ANM algorithms together. After the identity of a client is checked with InT and BIC, the ThreV algorithm works as follows. If the transmitted packet is greater than one within α, it rejects the request and considered as a spoofed frame. If the transmitted packet is equal to one within α, it is redirected to ANM. Thereby ANM algorithm checks the condition for start frame attack. The calculated CANM (Current ANM) gives 0.2 and the ANM is odd decimal, it will be redirected to TPatLetEn otherwise the transmitted packet is taken as an illegal one. If the transmitted packet is one at the time of α, ANM considers this as a legitimate user and process the request.

ThreV & ANM - Algorithm for Start frame Attack
Step 1: initialize α = 4ms, μ = 1, t = 0, i = 1.1
Step 2: if μ >1 && t< α then
Step 3: reject the packet, spoof and store it in InT
Step 4: if μ ==1 && t> α then
Step 5: goto ANM
Step 6: let D_{ANM} = i
Step 7: calculate C_{ANM}
Step 8: C_{ANM} = i + 0.2
Step 9: if C_{ANM} == odd_no&&$diff_{ANM}$ (C_{ANM} - P_{ANM}) gives 0.2
Step 10: request accepted and redirect to TPatLetEn
Step 11: else
Step 12: request rejected and store in InT
Step 13: if μ ==1 && t== α then
Step 14: process the request

Algorithm 2: ThreVANM for start frame attack over AP and Client

VII. Experimental Evaluation of Proposed Algorithms

This section discusses the results of the experiments performed with proposed solution applied to prevent DoS attacks. Experimental results show that the proposed ANM can effectively defend substantially against start frame and logoff frame attack. Experimentation is simulated on NS2 using four nodes such as client, intruder, AP and monitoring node, which are created for the study. Start frame over AP/Client and logoff frame over AP/Client are engaged to evaluate the performance of ANM algorithm. Experimental setup is tabulated in below Table 1.

A. ANM in Start Frame Attack Over AP/Client

Start frame attacks are experimented and the solution is applied to evaluate the performance of the proposed algorithm. 80 CBR packets are taken for the experimentation on start frame attack with the duration of 50 seconds using TCP agent. ANM offers a reasonably good result when compared with the time of start frame attack but in attack over the client, packet delivery ratio

decreased when compared to attack over AP. Further, we extend this work to hybridize multiple techniques to carry out the experiments on preventing DoS attacks as a future work.

Table 1. Experimental Setup

Area	500 ×500
Packet type	CBR
Packet Size	1000
CBR interval	0.008
Duration of Simulation	50 secs
Nodes	4 nodes (1 Client, 1 AP, 1 Attacker and 1 Monitoring node)
Queue type	Drop tail
Queue limit	10
MAC type	MAC 802.11
Channel	Wireless
Bandwidth	1.7 Mb
Agent	TCP

Table 2. Result of Start Frame Over AP/Client

Parameter	Over Client		Over AP	
	Attack Scenario	ANM	Attack Scenario	ANM
Packet Delivery Ratio	61.53	93.97	73.03	77.5
Control Overhead	81	78	101	50
Normalized Overhead	1.687	1.141	1.55	0.80
Delay	0.16	0.05	0.25	0.20
Throughput	177688	479035	429829	938839
Packet drop	30	5	24	18

B. ANM in Logoff Frame Attack over AP/Client

83 CBR packets were taken to experiment logoff attack over AP/Client. ANM produces better result than an attack scenario. Packet delivery ratio and throughput were increased in a good manner and control overhead, normalized routing overhead, delay and packet drop were decreased which imply that ANM is an effective solution in defend against logoff frame DoS attack.

C. ThreVANM in Start Frame And Logoff Frame Attack

The same experimental scenario was setup to evaluate the attacks and employ our ThreVANM algorithm. Start frame attack uses 82 CBR packets uses TCP agent for client and AP communication. Attacker node uses UDP null agent which has no acknowledgement. By comparing ANM with the proposed hybrid algorithm ThreVANM, hybrid algorithm yields comparatively good result except the throughput of the network. It is clearly indicated in the table 4.

81 CBR packets are taken to evaluate the logoff frame attack. The network performance is observed and recorded during the logoff frame attack and after implementing ThreVANM. The proposed ThreVANM produces effective result than ANM which is the main objective of this work. Performance of packet delivery ratio and control overhead are decreased when compared with ANM but gives reasonable result.

Table 3. Result of Logoff Frame Over AP/Client

Parameter	Over Client		Over AP	
	Attack Scenario	ANM	Attack Scenario	ANM
Packet Delivery Ratio	79.48	93.97	89.15	90
Control Overhead	98	89	108	63
Normalized Overhead	1.58	1.14	1.5	0.85
Delay	0.34	0.25	0.22	0.20
Throughput	554613	479035	495437	606485
Packet drop	16	5	9	4

Table 4. Result of Start Frame Over AP/Client

Parameter	Over AP		Over Client	
	Attack Scenario	ThreV ANM	Attack Scenario	ThreV ANM
Packet Delivery Ratio	61.53	95.06	73.03	91.56
Control Overhead	81	116	101	103
Normalized Overhead	1.6875	1.50	1.55	1.35
Delay	0.16	0.15	0.25	0.19
Throughput	277688	379948	429829	786794
Packet drop	30	4	24	7

Table 5. Result of Logoff Frame Over AP/Client

Parameter	Over AP		Over Client	
	Attack Scenario	ThreV ANM	Attack Scenario	ThreV ANM
Packet Delivery Ratio	89.15	95.06	79.48	88.75
Control Overhead	108	116	98	102
Normalized Overhead	1.5	1.50	1.58	1.43
Delay	0.22	0.15	0.34	0.17
Throughput	495437	379948	554613	578122
Packet drop	9	4	16	9

VIII. Results and Discussion

This section discusses the experimental results of the proposed solution which are carried out to prevent DoS attacks. Start frame and logoff frame attack is evaluated based on packet delivery ration, packet drop, normalized routing overhead, control overhead, delay time and throughput. Performance of the ANM is evaluated as given below.

A. Evaluation of ANM in DoS Attack

ANM achieves good result in packet delivery ratio when compare with logoff frame and start frame attack. ANM performs well in logoff frame attack. Fig 2 shows that the Packet delivery ratio is decreased in start frame attack over AP than the attack scenario of logoff frame attack over Client. During the start frame attack over AP and Client packet delivery ratio is decreased whereas it is increased after implementing ANM mechanism. ANM produces promising result in start frame attack over AP/Client than logoff frame attack which gives effective result than ThreV algorithm.

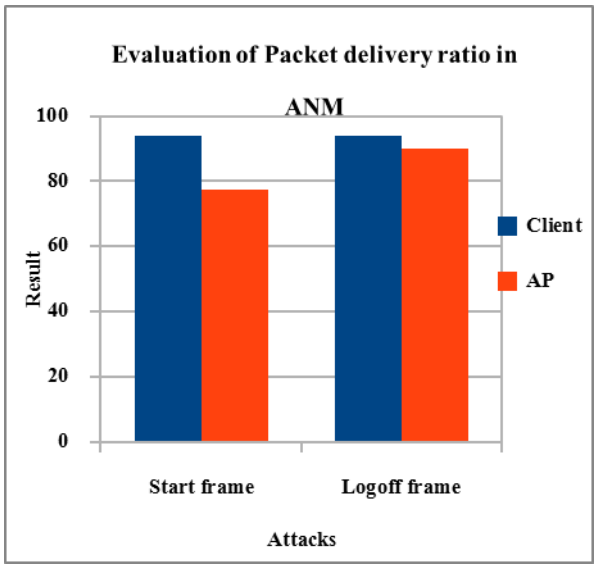

Fig 2. Packet delivery ratio using ANM

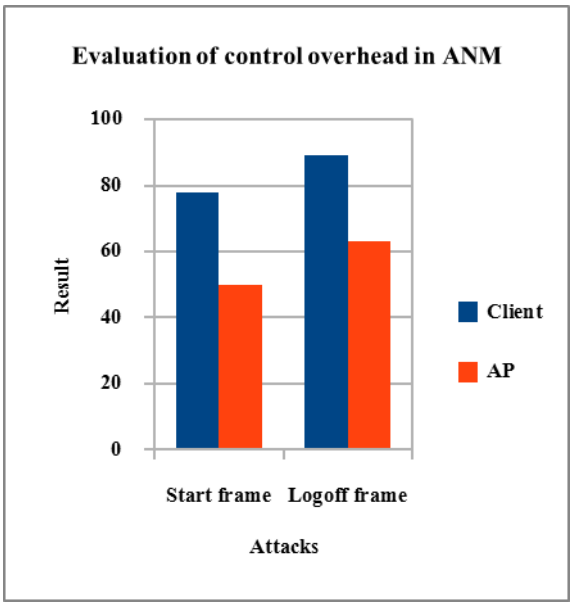

Fig 3. Result of Control overhead in ANM

By implementing ANM, control overhead is much decreased than all other types of attacks which are as depicted in Fig 3.

In case of delay time, ANM gives best result in start frame attack over Client which gives 0.05 as a delay time whereas logoff frame over AP produces 0.20 as a delay time which is higher than the start frame attack but a reasonable one. It is shown clearly in Fig 4 Start frame attack over AP gives a best throughput among all other types of attack than the ThreV algorithm. It is observed that proposed ANM effectively defend against start frame and logoff frame attack when compared with attack scenario.

The Fig 5 shows the evaluation of throughput by using the ANM. The throughput is measured when the attack is over the Client and the attack is over the AP.

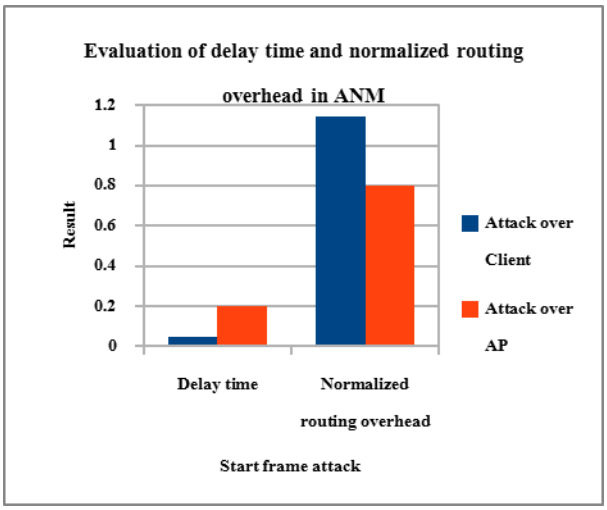

Fig. 4. Performance of ANM in delay time and normalized routing overhead

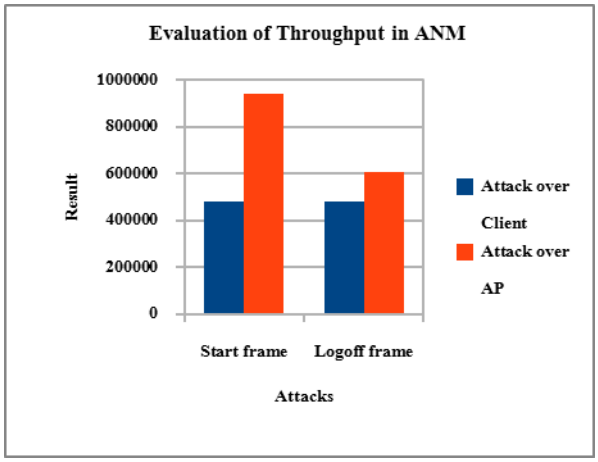

Fig 5. Evaluation of throughput in ANM

B. Evaluation of ThreVANM in DoS Attack

To enhance the performance of the proposed algorithm which is developed by integrating ANM and ThreV and its performance were measured. By combining ThreV and ANM, the algorithm produces effective result in packet delivery ratio, delay time and packet drop. Moderate decreases in control overhead, normalized routing overhead and throughput. Increases number of control overhead and normalized routing overhead shows that the ThreVANM fails to perform well in this case. This could be overcome by combining this with TPatLetEn mechanism. ThreVANM gives best result in start frame and logoff frame attack over AP than the client which is good result when compared with ThreV and ANM. Fig 6 and 8 shows the packet delivery ratio, delay time and normalized routing overhead which is obtained from the proposed ThreVANM.

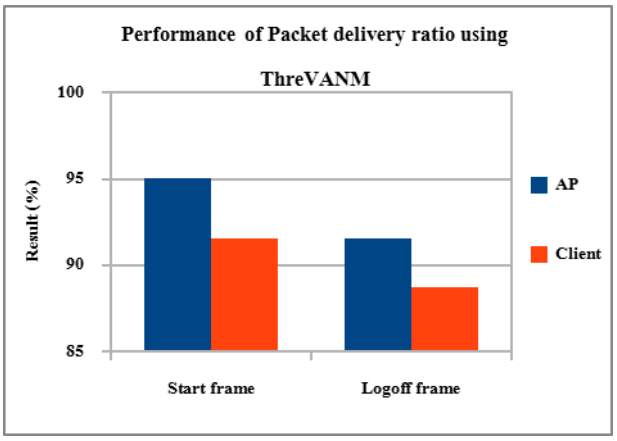

Fig. 6. Packet delivery ratio after implies ThreVANM

The Fig 7 shows that the packet drop is decreased after implementing ThreVANM. Effective result is obtained in start frame and logoff frame attack over AP. Delay time is decreased in start frame over AP. By analyzing ThreVANM, it performs well in both the attacks. In normalized routing overhead, start frame attack over client gives promising result.

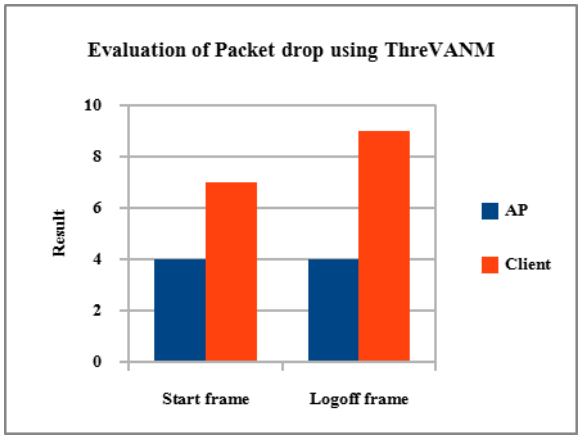

Fig 7. Evaluation of packet drop after implements ThreVANM

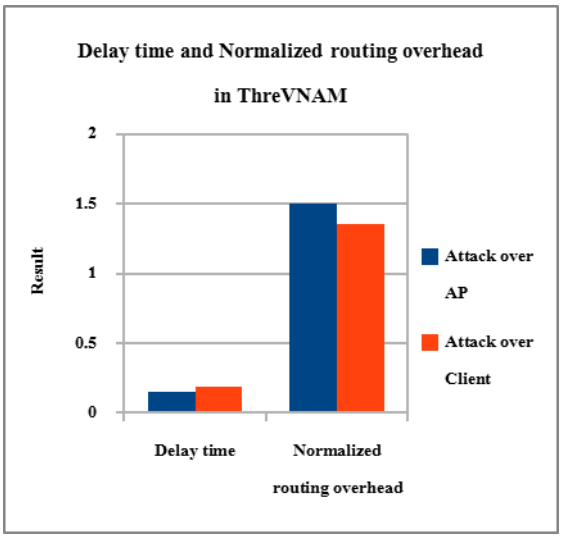

Fig. 8. Delay time and normalized routing overhead using ThreVANM

Delay time and normalized routing overhead is measured after implementing ThreVANM. The above Fig 8 shows that the ThreVANM produces better results in preventing the attack from both the Client side and AP side.

IX. Conclusion

This paper proposes ANM algorithm and hybridization of ThreV with ANM. By comparing the results obtained, it is evident that the hybridized algorithm provides more security than the ANM mechanism unaccompanied. For the effective detection and prevention of the attack, the ThreVANM is found to be more effective. The effectiveness of the algorithm is measured by using the parameters such as packet delivery ratio, control overhead, normalized routing over head, delay time, throughput and packet drop. Due to the hybridization of the techniques like ThreV and ANM with each other, the control overhead and normalized routing overhead are observed to produce high than the ANM algorithm alone.

References

[1] Anjum, Farooq, Subir Das, Praveen Gopalakrishnan, Latha Kant, and Byungsuk Kim (2005) "Security in an insecure WLAN network." In *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on*, vol. 1, pp. 292-297. IEEE.

[2] Arash Habibi Lashkari, Mir Mohammad SeyedDanesh, BehrangSamadi (2009). A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i). *2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, Beijing, China, August 8-11, pp. 48-52.

[3] Bansal, R., Tiwari, S., &Bansal, D, (2008) "Non-cryptographic methods of MAC spoof detection in wireless LAN", In *Networks, 2008. ICON 2008*, pp. 1-6, IEEE.

[4] Brad Antoniewicz "802.11 attacks version 1.0", White paper.

[5] Cardenas, E. D. "MAC Spoofing-An Introduction": http://www. giac. org/practical."

[6] Durairaj M, Persia A (2014) "ThreV - An Efficacious Algorithm to Thwart MAC Spoof DoS Attack in Wireless Local Area Infrastructure Network", *Indian Journal of Science and Technology*. Vol 7 (5), 39-46.

[7] Ferreri F and Bernaschi M, Valcamonici L (2008). Access points vulnerabilities to DoS attacks in 802.11 networks. *Wireless Networks*,vol 14, pp. 159-169, 2008.

[8] Guo, F., &Chiueh, T. C., (2006) "Sequence number-based MAC address spoof detection", In *Recent Advances in Intrusion Detection*,pp. 309-329. Springer Berlin Heidelberg.

[9] http://en.wikipedia.org/wiki/IEEE_802.11w (2009).

[10] Jalil Desa, Mina Malekzadeh, Abdul Azim Abdul Ghani and ShamalaSubramaniam (2008). An Experimental Evaluation of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks. *International Journal of Computer Science and Network Security*, Vol. 8, No. 8, pp. 1-5.

[11] John Bellardo and Stefan Savage (2003). 802.11 denial-of-service attacks: real vulnerabilities and practical

solutions. *USENIX Security Symposium*, Washington D.C.
[12] Kai Tao, Jing Li, and SrinivasSampalli (2008)"Detection of Spoofed MAC Addresses in 802.11 Wireless Networks", Springer-Verlag Berlin Heidelberg pp. 201–213.
[13] Kemal Bicakci and BulentTavli (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*, pp. 931–941.
[14] Li, Qing, and Wade Trappe (2007) "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships." *Information Forensics and Security, IEEE Transactions on* 2.4: 793-808.
[15] Nancy Cam-Winget, Russ Housley, David Wagner and Jesse Walker (2003). Security flaws in 802.11 data link protocols. *Communications of the ACM*, Vol.46, Issue. 5.
[16] Radomir Prodanovic and DejanSimic (2007). A Survey of Wireless Security. *Journal of Computing and Information Technology*, CIT 15, 3, pp. 237-255.
[17] Stanley Wong (2003). The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards. *GSEC Practical* v1.4b.
[18] Tanatat Saelim, PrawitChumchu and ChunyamonSriklauy (2011). A New MAC Address Spoofing Detection Algorithm using PLCP Header. *IEEE, ICOIN*, 48-53.
[19] Yong Sheng, Keren Tan, Guanling Chen, David Kotz and Andrew Cambell (2008). Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength, *The 27th Conference on Computer Communications IEEE*.

Authors' Profiles

Dr. M. Durairaj is Assistant Professor in School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamilnadu. He completed his Ph.D. in Computer Science as a full time research scholar at Bharathidasan University on April, 2011. Prior to that, he received master degree (M.C.A.) in 1997 and bachelor degree (B.Sc. in Computer Science) in 1993 from Bharathidasan University. His Ph.D. work was to study different possibilities and device a methodology for hybridizing two Machine-learning techniques for making an effective prediction system for processing clinical / medical data. At present, he is Assistant Professor in Computer Science at Bharathidasan University, prior to this he was Research Associate at National Research Centre on Rapeseed-Mustard (Indian Council of Agricultural Research) for 12 years. He has 40 publications in his credit. His area of research includes Data Mining, Soft Computing, Cloud Computing and Big Data Analytics.

Persia. A is a Ph.D., Full Time Scholar in the School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India. She is presently working on Denial of Service attacks. She has published 13 research papers in International Conferences and Journals and also presented 3 papers in National Conferences.

How to cite this paper: Durairaj M, Persia A,"ANM to Perceive and Thwart Denial of Service Attack in WLAN", IJCNIS, vol.7, no.6, pp.59-66, 2015.DOI: 10.5815/ijcnis.2015.06.07

