SNAuth-SPMAODV: Secure Neighbor Authentication Strict Priority Multipath AODV against Denial of Service attack for MANET in Military Scenario

[1]D.Devi Aruna [2]P.Subashini, PhD.

[1]Research Scholar, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore
[2]Associate Professor, Department of Computer Science, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore

ABSTRACT
A mobile ad-hoc network (MANET) is a peer-to-peer wireless network where nodes can communicate with each other without infrastructure. Due to this nature of MANET; it is possible that there could be some malicious and selfish nodes that try to compromise the routing protocol functionality and makes MANET vulnerable to Denial of Service attack in military communication environments. This paper consider military scenarios and evaluate the performance of Security-enhanced-Multipath AODV (Ad hoc On-demand Distance Vector Routing) routing protocol called SNAuth-SPMAODV (Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing). The protocol discovers multiple paths between sender and receiver nodes without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET.The SNAuth-SPMAODV protocol has been implemented and simulated on Qualnet 5.0. Based on the simulation result, it can be shown that SNAuth-SPMAODV does provide a more reliable data transfer compared to the normal AODV if there are malicious nodes in the MANET.

Keywords
MANET,AODV, Denial of Service attack,Strict priority algorithn,Secure neighbor authentication.

1. INTRODUCTION
Recent years Mobile ad hoc Networks start gaining attention from the industrial and academic research community due to their wide deployment and inherent nature of solving practical real world applications[1][4].The ease of deployment without the existing infrastructure makes ad hoc networks an attractive choice for dynamic situations such as military operations, disaster recovery, and so forth. Especially, military communication environments have been considered as one of the original motivations for MANET, due to the need for battlefield survivability and rapid deployment of self-organizing mobile infrastructure. These papers consider military ad hoc networks and conduct a performance analysis of proposed method for routing in conventional ad hoc networks.

The rest of this paper is organized as follows. Section 2 gives Review of Literature Section 3 briefly describes problem statement Section 4 discusses proposed methodology. Section 5 describes Simulation model.

2. REVIEW OF LITERATURE
This chapter briefly describes denial of service attack and routing protocols for MANETS.

2.1 Denial of Service attack
An attacker attempts to avoid authorized and legitimate users from the services offered by the network. The typical way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operate in the manner in which it is designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. DoS attacks can be launched against any layer in the network protocol stack. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service. For example, consider the following: In figure1 assume a shortest path that exists from S to X and C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet towards X with the source route S --> A --> B --> M --> C --> D --> X contained in the packet's header. When M receives the packet, it can alter the source route in the packet's header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful [2][3].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1: Denial of Service attack

2.2 Route Selection
Proactive routing protocols generate routes and store them for later use. On- demand routing protocols only generate routes when necessary. The latter is used more often in MANETs because they require fewer resources. The mostly used on-demand routing protocols are Ad-hoc On-demand Distance

Vector (AODV) Unless modified, the protocol use single routes between sender and receiver nodes. Multipath routing reduces dependency on single nodes and routes, offering robustness in a secured MANET.

2.2.1 Adhoc On demand Routing protocol (AODV)

AODV routing protocol is based on DSDV and DSR algorithm and is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated [4]. This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [7][8][9]. In general, the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Figure2 depicts the traversal of control messages.

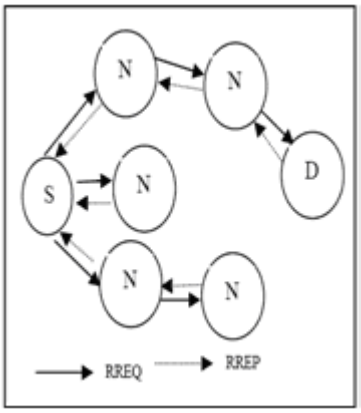

Figure2: Traversal of Control Messages

2.2.2 Multipath Routing

Ad-hoc wireless routing protocols like AODV are mainly designed to discover and use a single route between a sender and receiver node. However, multiple paths between sender and receiver nodes can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth.

Several multipath routing protocols based on DSR have been proposed, such as Split Multipath Routing (SMR) and Multipath Source Routing (MSR). Each of these multipath routing protocols broadcast data over all paths simultaneously. This technique has all the advantages previously mentioned, but it also introduces more packets into the MANET.

2.3 Strict-Priority Routing

Multiple paths is used in ad-hoc networks to achieve higher bandwidth is not as straightforward as in wired networks. Because ad-hoc networks communicate over a wireless medium, radio interference may be a factor when a node communicating along one path interferes with a node communicating along another path, limiting the achievable throughput. Still, simulations have shown that broadcast multipath routing creates more overhead but provides better performance in congestion and capacity than unipath routing, provided the route length is within a certain upper bound which is derivable. Additionally, the proper selection of routes using a strict priority multipath protocol can increase further the network throughput.

2.4 Secure Neighbor Authentication

The secure neighbor authentication has two variants. The first variant is based on pair-wise shared secrets, and the second variant is based on certification.

In secure neighbor authentication (SNAuth), every mobile node establishes an authenticated neighborhood on the move. Periodically, every mobile node X broadcasts its identity packet <SNAuth- HELLO, X> to its neighborhood.

1. In the pair-wise shared secret variant of SNAuth, Y, a neighboring receiver of the identity broadcast initiates a 3-way challenge-response handshake to authenticate X, the sender of the identity broadcast.

a. Suppose X and Y share a pair-wise secret k. Now Y selects a random nonce n1, encrypts n1 with k, sends the encrypted result ENCk (n1) to X by a message <CHALLENGE, Y, ENCk (n1)>.

b. If the receiver of the challenge message is indeed X, then it can decrypt ENC k (n1) and sees n1. X selects another random nonce n2, encrypts ENCk (n1 XOR n2), and sends back <RESPONSE1, X, n2, ENCk (n1 XOR n2)> as the response to the challenger Y.

c. When Y receives the response, Y decrypts ENCk (n1 XOR n2) and obtains n1 XOR n2. If Y can get the same result from XORing n2 in the response and its own challenge n1, then X passes the test with success. Otherwise, Y does not send any packet to X and does not receive packets from X except the response packets, until a correct <RESPONSE1> packet from X can pass the test. Upon detecting a success, Y puts X in its secure neighbor list. Y selects a random nonce n3 and sends out a confirmation response <RESPONSE2, Y, n3, ENCk (n1 XOR n2 XOR n3)> to X.

d. Upon receiving the RESPONSE2 message, X decrypts ENCk (n1 XOR n2 XOR n3) and obtains n1 XOR n2 XOR n3. If this matches the result of XORing n1 that is previously decrypted, its own n2 and n3 in the RESPONSE2 packet, then X inserts Y into its secure neighbor list. (This three-way handshake is required because X needs to verify that Y actually knows k)

e. End of the challenge-response protocol. Figure 3 shows Challenge-Response Protocol-Three way handshake

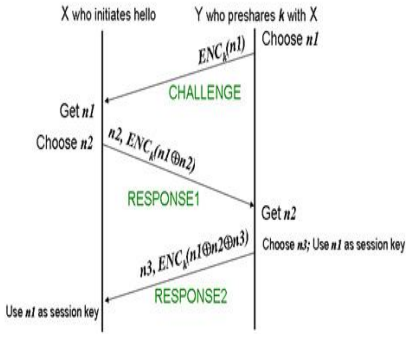

Figure 3: Challenge-Response Protocol-Three way handshake

In the above description, all nonce length is currently set to 128-bit long. Encryption block length is 128-bit. Key k can be 128-bit, 192-bit, or 256-bit. Session key means that the key n1 is used until the time when the next HELLO received by Y from X successfully passes the test again.

2. A a little different challenge-response scheme is used if Y does not pre-share a master secret k with X. Here X must broadcast its certificate CERTx = [X, certified public key PKx, certificate valid time] in a CERTIFIED_HELLO message. For Y's CHALLENGE, Y uses PKx to encrypt n1 and obtains ciphertext PKx (n1). Y must also add its own certificate CERTy = [Y, certified public key PKy, certificate valid time] and sign the entire message with its own private key SKY. It recommend the public key cryptosystem in use be an Elliptic Curve Cryptosystem (ECC), because ECC features shorter certificate length and ciphertext length, thus incurring less communication overhead. Figure 4 shows Three Way Challenge-Response Handshake.

As depicted below, there are a number of computational changes, and RESPONSE2 is spared, but the RESPONSE message format is unchanged.

Figure 4: Three Way Challenge-Response Handshake

When every neighboring receiver of X finishes the authentication and key-agreement process, node X obtains a secure snapshot of its neighborhood. In the neighborhood, every other node is authenticated and shares an IPsec security association with the node X. As the SNAuth protocol runs on every mobile node, the statement is true if node X is replaced with any node X'.

3. PROBLEM STATEMENT

This research investigates how to integrate security policies of a MANET with secure neighbor authentication that will allow the MANET to function securely in a military environment without degrading network performance. The specific problem to be addressed is how to use secure neighbor authentication of nodes in a multipath routing algorithm in MANET protected from Denial of service attack in military environment. Most of such performance analysis are normally done on commercial settings. For instance, wireless LAN technologies in the 2.4 GHz ISM frequency band are generally assumed, offering data rates up to 2 Mbps within the range of 250 m. This paper is motivated by the observation that such propagation and network models assumed by the current ad hoc networking simulations are quite different from real world military environments. In fact, a few hundred MHz frequency band (i.e., VHF or even HF) is used with very low data transmission rates (e.g., 384 Kbps) for the military scenarios [15]. Table I summarizes these differences in terms of a physical layer model. Networking environments such as network size, nodes' mobility model, and traffic patterns are quite different as well. For instance, the size of military networks is often far greater than that of their conventional counter parts both in the number of nodes and dimensions of the geographical areas.

Table I: physical layer model for military environments

Parameters	**Military devices**	**Conventional devices**
Frequency	30, 88, 300 *MHz*	2.4, 5 *GHz*
Propagation limits	-115 *dBm*	-110 *dBm*
Radio propagation model	Two-ray ground	Line-of-sight
Data rates	9.6~384 *Kbps*	2~54 *Mbps*
Transmit power	37 *dBm*	15 *dBm*
Receive sensitivity	-100 *dBm*	-90 *dBm*

4. PROPOSED METHODOLOGY

A MANET is a collection of mobile routers that move dynamically in unpredictable directions. The links connecting the nodes are wireless and thus are not as dependable as wired links. The links are also susceptible to capacity constraints. A MANET environment is characterized by numerous security threats because the wireless links are vulnerable to Denial of

service attack. The proposed method reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes it has the advantages of a multipath protocol without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in military environment.

5. SIMULATION MODEL

Using the QualNet network simulator [7], comprehensive simulations are made to evaluate the protocol. Qualnet provides a scalable simulation environment for multi-hop wireless ad hoc networks, with various medium access control protocols such as CSMA and IEEE 802.11. channel and physical layer settings are modified to apply more realistic military scenarios. Note that PRC-999K device is used as a reference model. 802.11 DCF and UDP protocols are used for MAC and a transport protocols, respectively. Also, CBR traffic is utilized in the study. As the TCP-based application protocols such as telnet or FTP show unstable performance in mobile wireless communication, it can not evaluate precise performance of routing protocol itself. CBR application model sends one packet per second, which represents relatively low traffic patterns in military environments. Each packet size is 512 Bytes. In military environments, operational network size is very large as compare to conventional case. Nodes in the simulation are assumed to move according to the "random way point" mobility model. Pause time is fixed to 20 seconds. The attackers are positioned around the center of the routing mesh in all experiments.

To evaluate the performance of proposed method by 4 measurements: Packet delivery radio, average end-to-end delay, routing overhead and Throughput.

6. RESULTS AND ANALYSIS

In this set of simulations, analyze performance of SNAuth-SPMAODV when the network size varies from 100 nodes to 1400 nodes. The network sizes and the respective network areas are shown in Table2 (approximately a walking Speed of soldiers). The size and the area are selected such that the node density is approximately constant, to properly evaluate proposed method.. For each performance metric, we compare SP- SNAuth-SPMAODV and AODV.

Table2: Network sizes and areas.

Nodes	Flows	Area (m)
100	20	1400×1400
150	30	1700×1700
200	40	2000×2000
250	50	2200×2200
300	60	2450×2450

Packet Delivery Ratio: Figure 5 shows the PDRs of Normal AODV, AODV under attack and SNAuth-SPMAODV. As the network density increases, there is an increase of radio interferences and collisions between nodes due to hidden/exposed terminals.SNAuth-SPMAODV show high PDRs are observed even for networks with more than 1000 nodes compared to AODV. For all network sizes from 100 nodes to 1400 nodes, SNAuth-SPMAODV consistently delivers about 5-10% more data packets than AODV.

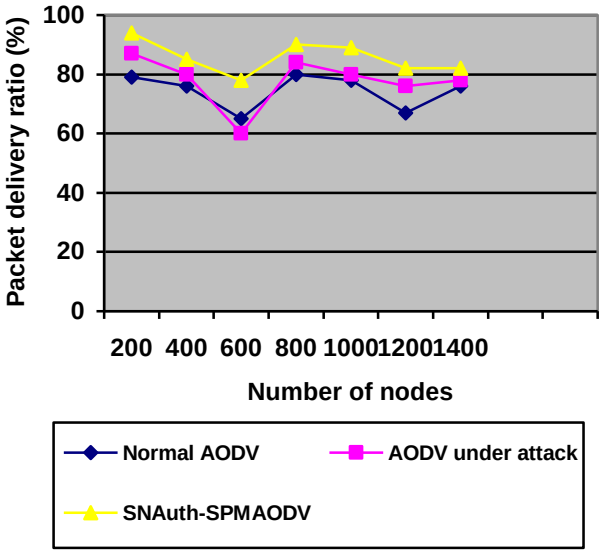

Figure5-SNAuth-SPMAODV-Packet Delivery ratio

Throughput: Figure 6 shows the throughput of Normal AODV, AODV under attack and SNAuth-SPMAODV. SNAuth-SPMAODV show high throughput even for networks with more than 1000 nodes compared to AODV.For all network sizes from 100 nodes to 1400 nodes, SNAuth-SPMAODV consistently delivers about 5-10% more throughput than AODV.

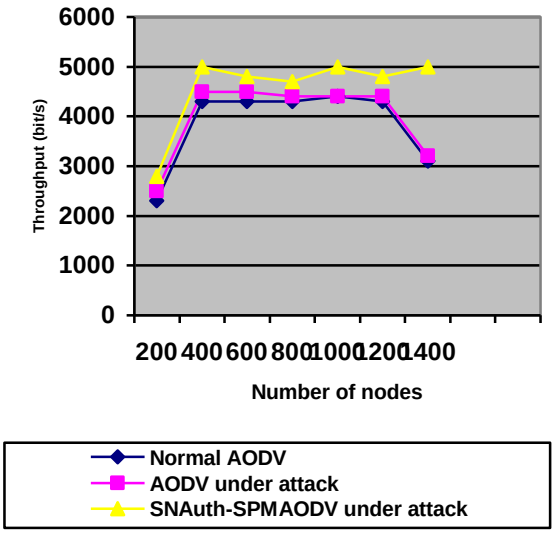

Figure 6-SNAuth-SPMAODV-Throughput

End-to-End Delay:Figure 7 shows an average end-to-end delay of SNAuth-SPMAODV and AOD according to the increase of network density. As the density of network becomes high, the probability of collision is also increases. For this reason, the average end-to-end delay rises as the network density becomes high in common. SNAuth-SPMAODV exhibits the lowest end-to-end delay most of the time. AODV has much higher end-to-end delay than proposed method.SNAuth-SPMAODV keep up good performance in delay as the network density becomes high.

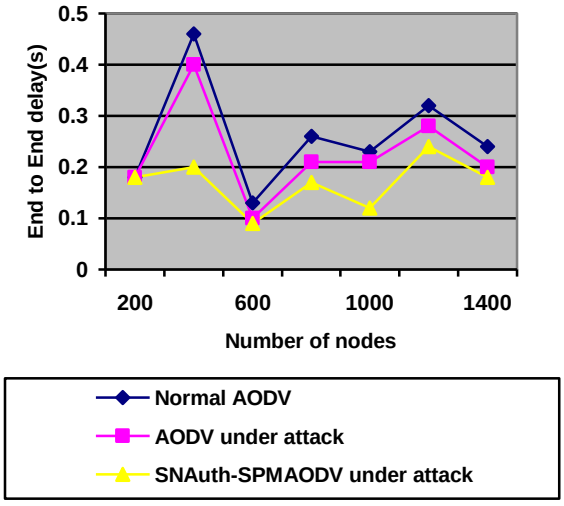

Figure7-SNAuth-SPMAODV-End to End Delay

Routing Overhead: The main purpose of using a hierarchy in MANETs is to reduce the routing overhead. Figure 8 shows the overhead of SNAuth-SPMAODV and AODV We observe that SNAuth-SPMAODV has much less routing overhead than AODV when the network size increases, whereas supporting high PDR (refer Figure 5). SNAuth-SPMAODV searches for a route whenever a need arises for it. Thus it show good performance in routing overhead.

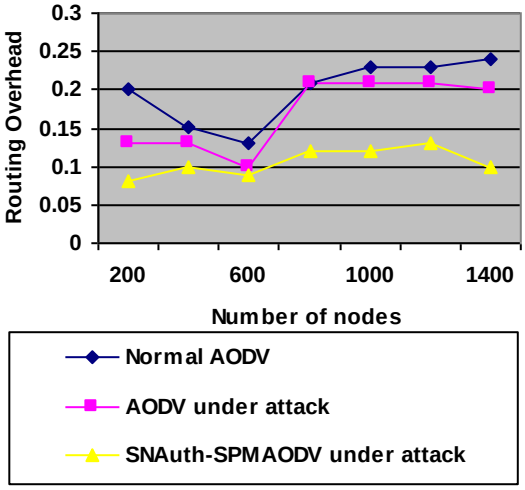

Figure 8-Routing Overhead

7. CONCLUSION

Mobile ad hoc networks (MANETs) can be applied to many situations without the use of any existing network infrastructure or centralized administration. In military environment, there is a need for the network to route packets through dynamically mobile nodes. MANETs can be considered as the solution for this highly mobile and dynamic military network. However it is not appropriate to directly apply conventional mobile ad hoc networks scheme to military network, since military communication system is different from conventional counter parts both in device's physical layer specification and networking environment. Therefore consider these particularities of military communication system to out simulation, and evaluate the performance of proposed method on the assumed military environment. In simulation results, SNAuth-SPMAODV provide good performance with every measurement metric in high network density environment.

8. REFERENCES

[1] B. Aerobic, R. Curtmola, H. Rubens, D. Holmer, and C. Nita-Rotaru, ***"****On the survivability of routing protocols in ad hoc wireless networks*," IEEE, 2005.

[2] Aad, J.P, Hubaux, and E.W. Knightly, "*Denial of Service Resilience in Ad Hoc Networks"*, ACM MOBICOM 2004, Philadelphia, PA, USA.

[3] V. Gupta, S. Krishnamurthy, and M. Faloutsos," *Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks****".*** In Proc. of MILCOM, 2002.

[4] C.E. Perkins, E.M. Royer & S. Das, *Ad Hoc On Demand Distance Vector (AODV) Routing, IETFInternet draft*, draft-ietf-manet-aodv-08.txt, March 2001

[5] A. Boukerche," Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks", Mobile Networks and Applications 9, Netherlands, 2004, pp. 333-342

[6] A.E. Mahmoud, R. Khalaf & A, Kayssi," *Performance Comparison of the AODV and DSDV Routing Protocols in Mobile Ad-Hoc Networks",* Lebanon, 2007

[7] Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available: Http:// Www.Scalablenetworks.Com/Products/Qualnet/Do wnlaod....

[8] S. Xu, Y. Mu, and W. Susilo. "*Secure AODV Routing Protocol Using One-Time Signature"***.** In *Proc. 1st International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2005)*. Springer, LNCS 3794. Dec. 2005.

[9] Ming Yu; Mengchu Zhou; Wei Su, ***"****A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments",* IEEE Transactions on Vehicular Technology Vol-58, Issue 1, Jan. 2009 , pp.449 – 460.

[10] Nasser, N.; Yunfeng Chen, "*Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks",* IEEE International Conference on Communications, ICC apos; Vol-07 , Issue 24-28 June 2007 , pp.1154 – 1159.

[11] M. G. Zapata. *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. IETF INTERNET DRAFT, MANET working group*, Nov. 2004. draft-guerrero-manet-saodv-02.txt.

[12] C. Perkins, E. B. Royer, S. Das, "*Ad hoc On-Demand Distance Vector (AODV) Routing - I*nternet Draft", RFC 3561, IETF Network Working Group, July 2003.

[13] C. E. Perkins and E. M. Royer, "*Ad-Hoc On Demand Distance Vector Routing",* Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, 1999, pp. 90-100.

[14] F. Bertocchi, P. Bergamo, G. Mazzin, *"Performance Comparison of Routing Protocols for Ad hoc Networks",* IEEE GLOBECOM 2003.

[15] Jong mu Choi and Young bae Ko. A Performance Evaluation For Ad Hoc Routing Protocols In Realistic Military Scenarios. In *Proceedings of The 9th CDMA International Conference*, October 2004.

9. ABOUT AUTHOR'S

Ms.D.Devi Aruna. received MCA Degree from Avinashilingam University for Women, Coimbatore in 2008 respectively and pursuing her Ph.D in same University. She has three years of research experience in UGC project. Her research interests are cryptography and Network Security. She has 17 publications at national and international level.

Dr. P. Subashini, Associate Professor, Dept. of Computer Science, Avinashilingam Deemed University have 19 years of teaching and research experience. Her research has spanned a large number of disciplines like Image analysis, Pattern recognition, neural networks, and applications to Digital Image processing. Under her supervision she has seven research project of worth one crore from various funding agencies like DRDO, DST and UGC.