Utilisation of DANGER and PAMP signals to detect a MANET Packet Storage Time Attack

Lincy Elizebeth Jim
RMIT University

Mark A Gregory
RMIT University

Abstract: The dynamic distributed topology of a Mobile Ad Hoc Network (MANET) provides a number of challenges associated with decentralised infrastructure where each node can act as the source, destination and relay for traffic. MANET's are a suitable solution for distributed regional, military and emergency networks. MANETs do not utilise fixed infrastructure except where connectivity to carrier networks is required and MANET nodes provide the transmission capability to receive, transmit and route traffic from a sender node to the destination node. In this paper, we present a Packet Storage Time (PST) routing attack where an attacking node modifies its storage time and thereby does not forward packets to the intended recipient nodes. In the Human Immune System, cells are able to distinguish between a range of issues including foreign body attacks as well as cellular senescence. This paper presents an approach using Artificial Immune System based Danger signal (DS) and Pathogen Associated Molecular Pattern (PAMP) signal to identify a PST routing attack.

Keywords: MANET; Packet Storage Time Attack; Artificial Immune System; Security, Danger Signal, Pathogen Associated Molecular Pattern

Introduction

A Mobile ad hoc Network (MANET) is formed by a group of mobile wireless nodes that do not require fixed infrastructure to maintain network connectivity (Giordano 2002). One of the many advantages of MANET is the absence of dedicated infrastructure to support packet forwarding and routing as each node acts as both host and router. MANET supports communications for military operations through to communications for the commercial sector including key roles in rescue or emergency scenarios (Loo, Mauri, & Ortiz, 2011). MANET can also be used to provide flexible education, health and business networks.

This autonomous nature of MANET makes it vulnerable to malicious active and passive attacks (Deng, Li & Agrawal 2002), and every node must be designed and built with the capability to respond to direct or indirect adversarial events. The mobility characteristics of

http://doi.org/10.18080/ajtde.v5n2.100

the ad hoc network facilitate independent management and control whilst part of one or more networks and this flexible design provides an opportunity for nodes to be compromised and affect the overall operation and efficiency of MANETs.

Based on the route discovery mechanism, the routing protocols in MANET can be classified into reactive or proactive (Mbarushimana & Shahrabi, 2007). Route discovery is initiated whenever there is a packet at a node in need of a route to the next node in the path to the destination node. Proactive routing protocols such as table-driven protocols are proactive where routes are computed beforehand and stored in the routing table so that routes will be readily available whenever any packet has to be transmitted.

In this paper, a detection system based on an Artificial Immune System (AIS) is proposed to detect ambushed or compromised nodes. The proposed framework utilises the principles of a dendritic cell algorithm which in turn mimics the Human Immune System (HIS), which has evolved into a sophisticated protector of the human body.

This paper is organised in the following five sections. Section 2 details key attack approaches found in existing in ad hoc networks and a brief overview of AIS. Section 3 provides the AIS based detection scheme. Sections 4 and 5 analyse the detection scheme and Section 6 contains the conclusion and work for future study.

MANET Attack Types

Security attacks on nodes in a MANET can be classified as either active or passive. Passive attacks involve snooping on the data exchanged in the network and often without the intention of altering the traffic. Passive attacks are very difficult to detect, because the network operation is not affected and they gather information about the network or pry on the communications between two or more nodes. This type of an attack may lead to an active attack if information gathered leads to an opportunity that would provide a positive outcome for the attacker. In passive attack a key facet that is the confidentiality of the network can be compromised.

In active attacks, the attacker alters the data being exchanged in the network thereby disrupting the normal functioning of the network and may launch an intrusive attack on a node (Deng & Agrawal 2002). The malicious behavior involves modification, injection or dropping packets and has a direct and immediate effect on network operation including affecting information security.

MANET nodes depend on battery power for operation and a loss of power efficiency may result from active attacks that lead to increased traffic (Perkins, 2008). Mobile nodes may

http://doi.org/10.18080/ajtde.v5n2.100

offer themselves as a relay node to forward data from other nodes in the network and providing a relay service can decrease the power available for the nodes use.

A brief description of the different types of attacks that occur in MANET is provided in the following sections.

Replay attack

In a MANET the topology changes permitting replay attacks where the attacker uses the strategy of storing control messages previously sent by a node (Adjih, Raffo & Muhlethaler, 2005; Goyal, Parmar & Rishi, 2011).

The attacker node resends the stored control messages which leads to genuine nodes updating their routing tables with stale information. This disturbs the normal operation of MANET.

Black hole attack

In a black hole attack the attacker node sends a false routing message claiming that it has the most conducive route to the destination, whereby leading all the genuine nodes to forward their packets to the attacker (Bala, Bansal & Singh, 2009; Mistry, Jinwala & Zaveri, 2010).

Flooding attack

In a flooding attack the attacker node sends multiple RREQ messages to a destination node that does not exist in the network (Bandyopadhyay, Vuppala & Choudhury, 2011; Yi, Dai, Zhang & Zhong, 2005).

As the destination node does not exist, none of the nodes will be able to send a Route Reply, leading to congestion and a network denial of service.

Wormhole attack

Wormhole attack is depicted in Figure 1. In this attack, the attacker nodes fabricate a route shorter than the original route, which in turn creates confusion amongst other nodes (Mahajan, Natu & Sethi, 2008). This attack is carried out by one or more nodes that create a tunnel between them whereby the attacker seizes packets and transmits to other nodes. The two colluding nodes send fake advertising messages that they have a single hop symmetric link between each other. These fake messages will be propagated to other nodes across the network thus compromising the shortest path routing calculations.

http://doi.org/10.18080/ajtde.v5n2.100

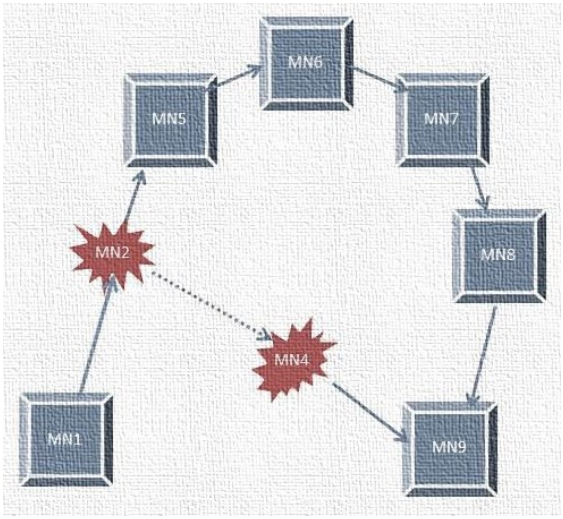

Figure 1 Colluding nodes in Wormhole Attack

The authors proposed a scenario where each node will keep track of the behaviour of its neighbours (Choi, Kim, Lee, & Jung, 2008). A RREQ message is sent by a node to the destination using its neighbour list. However, if the RREP is not received back within a stipulated time, the presence of a wormhole is identified and the route is added to the source node's wormhole list. Each node maintains a table which consists of RREQ sequence number and neighbour node identity. After sending a RREQ, the source node sets the Wormhole Prevention Timer (WPT) and waits until it overhears retransmission by the neighbour node. The maximum amount of time for a packet to travel a one-hop distance is WPT/2.

Artificial Immune Systems

AIS are intelligent and adaptive systems inspired by the human immune system toward real-world problem solving (Abdelhaq, Hassan & Alsaqour, 2011). AIS are adaptive intelligent systems "inspired by theoretical immunology and observed immune functions, principles and models, which are applied to complex problem domains" (Abdelhaq, Hassan, & Alsaqour, 2011).

A relatively recent immunological discovery known as Danger Theory now paves the way for designing more efficient, second generation AIS. The Dendritic Cell Algorithm (DCA) is a biologically inspired technique developed to detect intruders in computer networks (Abdelhaq, Hassan, Ismail, Alsaqour & Israf, 2011). The DCA is based on a metaphor of naturally occurring Dendritic cells (DCs), a type of cell which is native to the innate arm of the immune system (Abdelhaq, Hassan & Alsaqour, 2011). DCs are responsible for the initial detection of intruders, including bacteria and parasites, by responding to the damage caused by the invading entity. Natural DCs receive sensory input in the form of molecules, which can

http://doi.org/10.18080/ajtde.v5n2.100

indicate if the tissue is healthy, or in distress. These cells have the ability to combine the various signals from the tissue and to produce their own output signals. The output of DCs instructs the responder cells of the immune system to deal with the source of the potential damage. DCs are excellent candidate cells for abstraction to network security as they are the body's own intrusion detection agents.

The DCA is one of the most well-known Danger Theory contributions and utilises the role of the DCs in the HIS as forensic navigators and important anomaly detectors. DCs are defined as antigens presenting lymphocytes in the innate immunity; these lymphocytes play a key role in either stimulating or suppressing the adaptive immunity T-cells and hence controlling the immune system's response type.

DCA's capability as an anomaly detector algorithm inspires the use of a biological model to introduce a further DC inspired algorithm, which could detect other attack types in a MANET (Mazhar & Farooq, 2008; Abdelhaq, Hassan, Ismail & Israf, 2011). In addition, many of MANET's special characteristics and properties are similar to the innate immunity's abstract features; such as the openness and susceptibility of each to different types of attacks (Mazhar & Farooq, 2008).

AIS are increasingly being used to secure MANET because of its low communication and computational overhead (Gu, Greensmith & Aickelin, 2011). AIS based intrusion detection systems in MANET utilise the exemplar of discrimination between self and non-self. In this approach the system is first put in a learning phase, where the system learns the characteristics of a normal environment. Any changes that occur which do not match the normal environment are considered harmful. The problem with such an approach is limited fault detection. The behaviour of the normal environment during the learning phase cannot be taken as the prototype for trustworthy behaviour as a MANET environment keeps changing with time.

This approach becomes impractical once malicious nodes enter the network. As a result, identifying a valid route change due to mobility from a malicious node or advertisement of short routes by a malicious node can be challenging.

The properties of AIS (Mazhar & Farooq, 2008) such as being self-healing, self-defence and self-organising can be applied to meet the challenges of securing the MANET environment.

Proposed Attack-Packet Storage Time

Consider a MANET topology as shown in Figure 2, where the ad hoc network challenges to establish a route between the existing nodes is presented. In Figure 2, MN1 is the source

http://doi.org/10.18080/ajtde.v5n2.100

node and MN7 is the destination node. The intermediate nodes are MN2-MN6. In this scenario, consider the following available routes:

MN1-MN2-MN6-MN7

MN1-MN5-MN7

MN1-MN4-MN3-MN7

When a route is needed, the source node should take into account the battery power or energy of the participating nodes that provide a route reply.

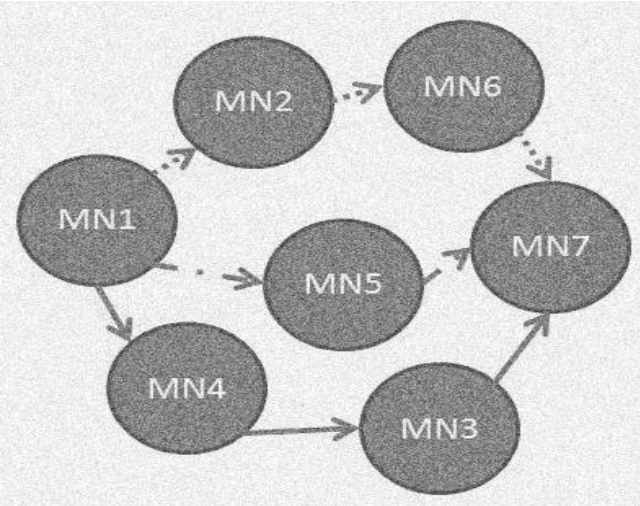

Figure 2 MANET scenario

In this scenario, a problem was identified where MN5 is an attacker/selfish node which does not want to expend energy to forward packets. This node is particularly interested in giving a RREP as it wants to maintain an updated routing table.

The Packet Storage Time (PST) attack is a novel concept introduced for the first time in MANET where each mobile node is incorporated with a buffer/queue. In this type of attack, the attacker modifies its own buffer/queue time to congest the network. When the packets are kept for a longer time than intended by each node, the packets become stale and the circulation of stale packets in the network leads to battery power wastage by the genuine nodes.

http://doi.org/10.18080/ajtde.v5n2.100

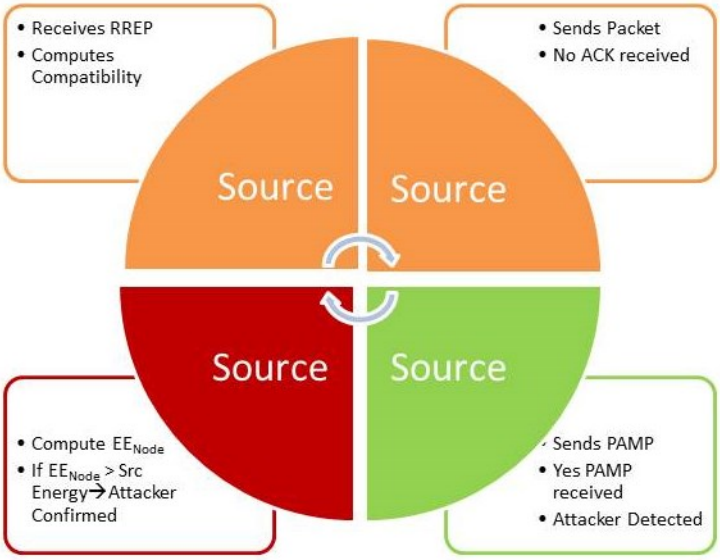

Figure 3 Proposed AIS algorithm

Proposed AIS Algorithm

A model based on the Danger Theory principle wherein each node is modelled as a DC is proposed. The presence or absence of danger is detected by the DC nodes, thereby identifying danger by indicating the presence of a malicious node. The DC nodes monitor the activity occurring in MANET to report any malicious node. The Pathogen Associated Molecular Pattern (PAMP) signal is utilised here to signify the presence of a malicious node in the network. Based on the concepts identified in the literature a mathematical model was constructed. The closer nodes should spend less energy to communicate. The battery life/energy of each DC node plays an important role while establishing routes. During route establishment, the energy of each node needs to be considered. Consider *n* to be an energy dependent variable. The energy associated with the source destination and intermediate nodes is assigned a weight which is dependent on the percentage of battery power that would be used during a route request and route reply communication. Based on above concept, the below given equation is formulated.

$$f(n) = \alpha n_s + \beta n_d + 2\gamma \bar{n} \quad (1)$$

where: $\alpha+\beta+\gamma=1$ and $\alpha, \beta, \gamma \in [0, 1]$ and $\bar{n}$ is the average of the energy among intermediate nodes, n_s is the source node energy, n_d is the destination node energy, α is the source node weight factor, β is the destination node weight factor, and γ is the intermediate nodes weight factor.

http://doi.org/10.18080/ajtde.v5n2.100

Consider the Effective Energy (EE) of Node *k*

$$\tilde{n}_k = F(n_k,h_k)=EE_{node(k)} = h_k * n_k \quad (2)$$

where h_k is the number of hops from node k to node s, and $F(n_k,h_k) \approx EE_{node(k)}$ should satisfy the postulates:

(1) If node *k* is far away from source node *s*, node *k* should have to take larger number of hops and more energy would be utilised which results in larger function value.
(2) If node *k* is closer to node *s*, node *k* should have to take lesser number of hops and lesser energy would be utilised which results in a smaller function value.

The effective mean energy of all the intermediate nodes is as follows

$$\tilde{n} = \frac{1}{m-2} \sum_{k=1,k\neq s,d}^{m} \tilde{n}_k \quad (3)$$

Combining (2) and (3) gives the Node Energy Momentous function

$$f(n)=\alpha n_s + \beta n_d + \frac{\gamma}{m-2} \sum_{k=1,k\neq s,d}^{m} h_k * n_k \quad (4)$$

From Eq (2) we get the Compatibility function

$$\hat{C}=1/F(n_k,h_k) \quad (5)$$

As Compatibility $\hat{C}$ increases the cost to establish the route between source and destination decreases which also implies that the node k has energy available for routing.

In a MANET, the source node initiates a route discovery whenever it should send a packet. The proposed Artificial Immune Systems Based Algorithm (AISBA) model consists of the following stages:

Normal

Consider the proposed AISBA model as shown in Figure 3. Initially the source initiates a route discovery in order to send a packet to a destination node and computes compatibility of the node from which it receives a RREP. The source node does not receive an acknowledgement (ACK) from the node that provided the RREP.

Attacker detection by using Danger Signal

When the source does not receive the ACK it activates its DC and sends a Danger Signal (DS); the good nodes acknowledge the Danger signal by sending Danger Signal received (DSrecvd). As the Danger Signal is not a priority signal there is no overwriting of the node buffer therefore the attacker node does not send back DSrecvd. This strategy is used when there is a smaller number of attacker nodes.

http://doi.org/10.18080/ajtde.v5n2.100

Attacker Detection

The source sends a high priority packet PAMP (high priority signal) message to the attacker node and the attacker node is forced to acknowledge receipt of the PAMP which indicates the presence of an attacker but this is not yet confirmed.

Attacker Confirmation

The source computes the node EE (EE_{node}) of the attacker node and compares the value with its own energy. If the EE_{node} happens to be greater than EE_{source} the presence of the attacker is confirmed.

The algorithm pseudo code is described as shown in Figure 4 and Algorithm 1. The source node broadcasts a RREQ and computes node compatibility for the nodes from which a RREP is received. The source node begins to send the packet and if an ACK is not received a high priority PAMP is sent. If the node is an attacker and it does respond with an ACK; this indicates the presence of the attacker node. The next step taken by the source is to compute the EE of the attacker, and a high EE value is used to confirm the presence of the attacker. This is also symbolically represented in the flowchart as shown in Figure 4.

Algorithm 1 Pseudo code of AISBA

1. Source Node broadcasts RREQ
   a) $Node_{src}$ broadcasts RREQ
   b) $Node_{intermed}$ sends RREP
2. Compute Compatiblity ($Node_{src}$,$Node_{intermed}$,Packet P)
   a) $Node_{src}$ computes compatibility of $Node_{intermed}$;
   b) **If** $Node_{src}$ sends packet and $Node_{src}$ does not receive Ack **then**
3. SendDS ($Node_{src}$, $Node_{intermed}$, DS_{send})
   a) $Node_{src}$ sends DS
   b) **If** $Nodei_{intermed}$ does not acknowledge DS **then**
   c) Detect if attacker or route error, do SendPAMP
4. SendPAMP ($Node_{src}$, $Node_{intermed}$,PAMPpacket PAMPp)
   a) $Node_{src}$ sends PAMP,
   b) **If** $Node_{intermed}$ acknowledges PAMP **then** attacker detected
5. Compute Effective energy of intermediate node ($EE_{nodeintermed}$)
   a) $EE_{nodeintermed}$ is computed by Source,

http://doi.org/10.18080/ajtde.v5n2.100

b) **If** $EE_{nodeintermed}$ >= $Node_{src}$, **then** presence of attacker is confirmed.

Simulation and Results

The ns-3.23 simulator was used to detect and confirm the presence of PST attacker using the AODV protocol. The simulation parameters used are shown in Table 1.

As can be seen in Figure 5 as the hop count increases in the network, the EE consumption by the mobile node is higher. As compatibility increases the cost to establish the route between the source and destination will decrease as can be seen in Figure 6. The route cost is a metric which is the ratio of transmitted control packets to the transmitted data packets. An increase in compatibility decreases the cost.

The average end-to-end delay (E2E) increases as shown in Figure 7 and during the PST as the attacker delays the packet whereas in an AISBA model the presence of an attacker is detected and confirmed thereby the packet will be forwarded via a routing path that does not contain the PST attacker. Hence the average E2E will be slightly higher for AISBA.

As can be seen in Figure 8, a PST attack causes packet loss to increase as the number of nodes increase, whereas with the AIS-based algorithm the packet loss is lower due to the proposed security improvement.

Table 1 Simulated Parameters

Simulator	Ns-3.23
Mobility Model	Random waypoint
Simulation Time	500s
Number of nodes	10-50
Traffic Type	UDP
Network Area	600m*600m
Mobility	6 m/s
Pause Time	5s
Transmission Range	50m

http://doi.org/10.18080/ajtde.v5n2.100

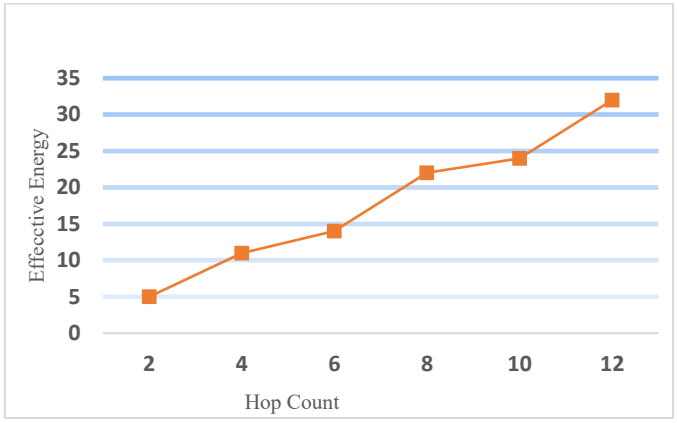

Figure 4 Effective Energy v/s Hop Count

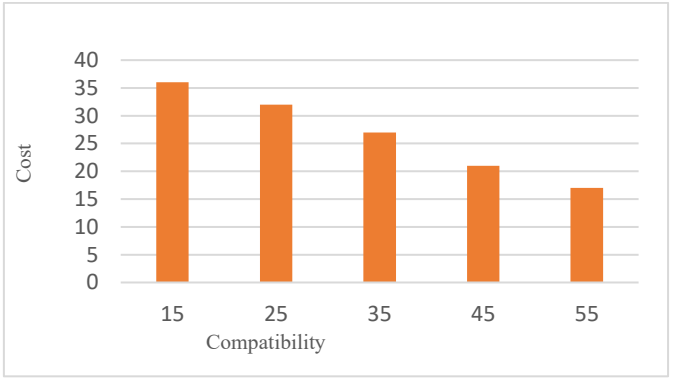

Figure 5 Compatibility v/s Cost

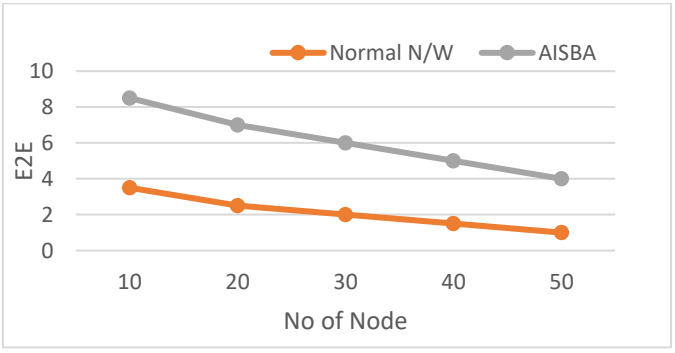

Figure 6 E2E v/s Number of nodes

http://doi.org/10.18080/ajtde.v5n2.100

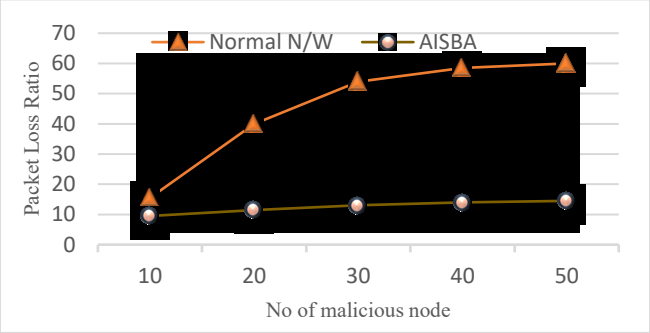

Figure 7 PST Attack-Packet loss v/s Number of nodes

Conclusion

In this paper, the PST attack is presented and the PST attack has been analysed using AIS principles and metrics including packet loss, delay and battery power. The solution proposed is robust and adopts AIS principles as an example of how AIS can be applied to MANET thereby reducing the effects of security events based on this attack type including inducing futile battery consumption. In future work, utilisation of a battery power metric with respect to the major nodes will be considered and will be included in the development of an improved security technique to increase MANET robustness.

References

Abdelhaq, M; Hassan, R; Alsaqour, R. (2011). *Using dendritic cell algorithm to detect the resource consumption attack over MANET*. Paper presented at the International Conference on Software Engineering and Computer Systems. https://link-springer-com.ezproxy.lib.rmit.edu.au/chapter/10.1007/978-3-642-22203-0_38

Abdelhaq, M; Hassan, R; Ismail, M; Alsaqour, R; Israf, D. (2011). Detecting sleep deprivation attack over manet using a danger theory-based algorithm. *International Journal of New Computer Architectures and their Applications (IJNCAA), 1*(3), 534-541. http://sdiwc.net/digital-library/detecting-sleep-deprivation-attack-over-manet-using-a-danger-theorybased-algorithm.html

Abdelhaq, M; Hassan, R; Ismail, M; Israf, D. (2011). Detecting resource consumption attack over MANET using an artificial immune algorithm. *Research Journal of Applied Sciences, Engineering and Technology, 3*(9), 1026-1033. http://www.airitilibrary.com/Publication/alDetailedMesh?docid=20407467-201109-201411110031-201411110031-1026-1033

Adjih, C; Raffo, D; Muhlethaler, P. (2005). *Attacks against OLSR: Distributed key management for security*. Paper presented at the 2005 OLSR Interop and Workshop.

http://doi.org/10.18080/ajtde.v5n2.100

https://www.researchgate.net/publication/242417041_Attacks_Against_OLSR_Distributed_Key_Management_for_Security

Bala, A; Bansal, M; Singh, J. (2009). *Performance analysis of MANET under blackhole attack*. Paper presented at the Networks and Communications, 2009. NETCOM'09. First International Conference on. http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/5384021/?reload=true

Bandyopadhyay, A; Vuppala, S; Choudhury, P. (2011). *A simulation analysis of flooding attack in MANET using NS-3*. Paper presented at the Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011. 2nd International Conference on. http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/5940916/

Choi, S; Kim, D.-y; Lee, D.-h; Jung, J.-i. (2008). *WAP: Wormhole attack prevention algorithm in mobile ad hoc networks*. Paper presented at the Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on. http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/4545782/

Deng, H; Li, W; Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications magazine, 40*(10), 70-75. http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/1039859/

Giordano, S. (2002). Mobile ad hoc networks. *Handbook of wireless networks and mobile computing*,325-346 http://au.wiley.com/WileyCDA/WileyTitle/productCd-0471419028.html

Goyal, P; Parmar, V; Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management, 11* (2011), 32-37. http://skirubame.ucoz.com/_ld/0/29_Topic_1-MANET_v.pdf

Gu, F; Greensmith, J; Aickelin, U. (2011). The dendritic cell algorithm for intrusion detection. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2824971

Loo, J. H; Mauri, J. L; Ortiz, J. (2011). *Mobile ad hoc networks: current status and future trends*: CRC Press. http://www.crcnetbase.com.ezproxy.lib.rmit.edu.au/doi/pdf/10.1201/b11447-1

Mahajan, V; Natu, M; Sethi, A. (2008). *Analysis of wormhole intrusion attacks in MANETS*. Paper presented at the Military Communications Conference, 2008. MILCOM 2008. IEEE. http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/4753176/?reload=true

Mazhar, N; Farooq, M. (2008). A sense of danger: dendritic cells inspired artificial immune systems for MANET security. *Proceedings of the 10th annual conference on Genetic and*

evolutionary computation. *Atlanta*, GA, USA, ACM: 63-70.
http://dl.acm.org.ezproxy.lib.rmit.edu.au/citation.cfm?id=1389105

Mbarushimana, C; Shahrabi, A. (2007). *Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks*. Paper presented at the Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on
http://ieeexplore.ieee.org.ezproxy.lib.rmit.edu.au/abstract/document/4224182/

Mistry, N; Jinwala, D. C; Zaveri, M. (2010). *Improving AODV protocol against blackhole attacks*. Paper presented at the Proceedings of the International Multi Conference of Engineers and Computer Scientists.
http://www.iaeng.org/publication/IMECS2010/IMECS2010_pp1034-1039.pdf

Perkins, C. E. (2008). Ad Hoc Networking 2001. *Boston, Adison-Wesley*.
https://www.pearsonhighered.com/program/Perkins-Ad-Hoc-Networking-paperback/PGM75272.html

Yi, P; Dai, Z; Zhang, S; Zhong, Y. (2005). A new routing attack in mobile ad hoc networks. *International Journal of Information Technology, 11*(2), 83-94.
http://www.intjit.org/cms/journal/volume/11/2/112_6.pdf

http://doi.org/10.18080/ajtde.v5n2.100