IJRRECS/March 2016/Volume-4/Issue-3/5404-5408 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

CONSIDERING EFFECT OF NOVEL ATTACKS ON ROUTING PROTOCOLS

T.Sai Priyanka[1], K.Pranathi[2], M.Amith Rajan[3], Dr.J.V.N.Ramesh[4]

[1,2,3] Student of Electronics and Computer Engineering, K L University, Guntur, A.P, India
[4]Associate Professor, Department of Electronics and Computer Engineering, K L University, Guntur, A.P, India

ABSTRACT:

In our work, we define Vampire attacks, which denote a novel class of resource consumption attacks that utilize routing protocols to block ad hoc networks by means of reduction of nodes' battery power. Vampire attacks are most general attacks of resource depletion where the energy which is consumed by network for composing and transmitting a message is superior when evaluated to that of an ordinary network. Traditional works on secure routing attempts to make sure those adversaries cannot make discovering of path for returning an unacceptable network path. Our work considers of attack-resistant minimal-energy routing, where adversary objective includes lessening energy savings. These attacks neither depend on flooding the network with huge amounts of data; however try to transmit as little data as promising to attain major energy drain, avoiding a rate limiting explanation. Vampire attacks interrupts functioning of a network instantly rather than work overtime to completely stop a network. These types of attacks are not dependant on exact protocols but to certain extent expose vulnerabilities in several accepted protocol classes. Vampire attacks are not specific to protocol, and do not depend on design properties of routing protocols, however rather make use of general properties of protocol classes.

Keywords: Adversary, Vampire attacks, Resource depletion attacks, Network.

1. INTRODUCTION:

Wireless ad-hoc networks offer one of missing connections among Internet and physical world. One of the most important exertions in sensor networks is the restricted power of nodes. Wireless ad hoc systems do not necessitate any predefined infrastructure for communication purpose which makes them appropriate for effortless deployment with negligible configuration as well as emergency situations. Wireless ad hoc networks experience from several attacks such as denial of Service, Reduction of Quality, Resource Depletion and Routing infrastructure attacks. Attacks of resource depletion affect continuing availability of network by completely depleting battery of node. Since wireless networks have become increasingly essential to daily functioning organizations, accessibility faults turn out to be less tolerable; consequently high availability of these networks is an important property, and have to hold even under malevolent conditions [1]. Vampire attacks are most general attacks of resource depletion where the energy which is consumed by network for composing and transmitting a message is superior when evaluated to that of an ordinary network. These attacks neither depend on flooding the network with huge amounts of data; however try to transmit as little data as promising to attain major energy drain, avoiding a rate limiting explanation [2][3]. Vampire attacks interrupts functioning of a network instantly rather than work overtime to completely stop a network. These types of attacks are not dependant on exact protocols but to certain extent expose vulnerabilities in several accepted protocol classes. In our work, we define Vampire attacks, which is a novel class of resource consumption attacks that make use of routing protocols to to block ad hoc networks by means of reduction of nodes' battery power.

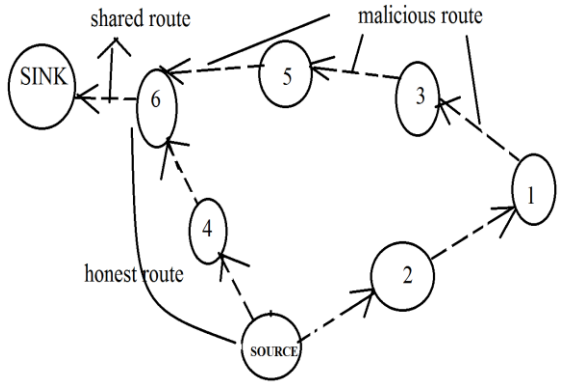

Fig1: An overview of fig specifying stretch attack

2. INTRODUCTION TO VAMPIRE ATTACKS:

Strength of the attack was measured by the ratio of network energy utilized in benign case to energy utilized in malevolent case.

Energy usage by malevolent nodes is not measured, as they can constantly unilaterally drain their own batteries. Adversaries are considered as malicious insiders and contain the comparable network access as honest nodes. Adversary location within the network is supposed to be unchanging and random, since if an adversary corrupts several honest nodes earlier than the network was deployed, and cannot manage their final positions. All routing procedures utilize not less than one topology discovery period, as ad hoc deployment imply no earlier position knowledge [4]. Vampire attacks are not specific to protocol, and do not depend on design properties of routing protocols, however rather make use of general properties of protocol classes. Traditional works on secure routing attempts to make sure those adversaries cannot make discovering of path for returning an unacceptable network path; however Vampires do not disrupt discovered paths, instead by means of existing convincing network paths. Protocols that make the most of power efficiency are also unsuitable, while they depend on cooperative node behaviour and cannot optimize out malevolent action. Transmission of a message that cause additional energy to be consumed by network than when anode of honest passed on a message of the same size to similar destination, while using different packet headers describes vampire attack. These attacks neither depend on flooding the network with huge amounts of data; however try to transmit as little data as promising to attain major energy drain, avoiding a rate limiting explanation. While Vampires utilize protocol-compliant messages, these attacks are extremely hard to notice and put off.

3. OVERVIEW OF VARIOUS ATTACKS:

Vampire attacks interrupts functioning of a network instantly rather than work overtime to completely stop a network. Attackers will construct packets which pass through more hops than essential, thus even if nodes spend least necessary energy to transmit packets, each packet is more pricey to convey in presence of Vampires. Our work considers of attack-resistant minimal-energy routing, where adversary objective includes lessening energy savings. In carousel attack, an adversary conveys a packet by series of loops, in order that the same node appears in route numerous times. This approach can be used to enhance the route length away from

the several nodes in network, merely limited by approved entries within source route. In carousel attack an adversary composes packets with intentionally initiated routing loops. Carousel attack sends packets in circles and target source routing protocols by means of using restricted verification of message headers at forwarding nodes, allow a single packet to constantly traverse the similar set of nodes. Stretch attack as shown in fig1 is another attack in same vein where a malevolent node build artificially long source routes, cause packets to traverse a larger than best possible number of nodes [5]. Source and sink are significant; the stretch attack can attain same efficiency autonomous of the attacker's network position comparative to the destination, thus worst case effect is far more probable to take place. Recent works in minimal-energy routing, aims to enhance the duration of power-constrained networks by means of less energy to transmit as well as receive packets is equally orthogonal: these protocols spotlight on cooperative nodes and not malevolent scenarios. Vampires will enhance energy usage even in situations of minimal-energy routing and when MAC protocols of power conserving are used; these attacks cannot be prohibited at MAC layer. These attacks will be less effectual in hierarchical networks, where nodes transmit messages towards aggregators, who consecutively send it to other aggregators, which send it towards a monitoring point. The carousel attack is prohibited by having forwarding nodes check source routes meant for loops. The stretch attack is additionally demanding to prevent and its success rests on forwarding node not examining for optimality of route. In stretch attack, targeting source routing, an opponent put up artificially long routes, potentially traversing each node within the network. Stretch attack, increases packet path lengths, causes packets to be processed by several nodes that are autonomous of hop count all along shortest path among adversary [6].

4. CONCLUSION:

In our work, we define Vampire attacks, which is a novel class of resource consumption attacks that make use of routing protocols to block ad hoc networks by means of reduction of nodes' battery power. Vampire attacks are not specific to protocol, and do not depend on design properties of routing protocols, however rather make use of general properties of protocol classes. These types of attacks are

not dependant on exact protocols but to certain extent expose vulnerabilities in several accepted protocol classes. Adversaries are considered as malicious insiders and contain the similar network access like honest nodes. Wireless ad hoc networks experience from several attacks such as denial of Service, Reduction of Quality, Resource Depletion and Routing infrastructure attacks. Vampire attacks are most general attacks of resource depletion where the energy which is consumed by network for composing and transmitting a message is superior when evaluated to that of an ordinary network. Our work considers of attack-resistant minimal-energy routing, where adversary objective includes lessening energy savings. Vampire attacks interrupts functioning of a network instantly rather than work overtime to completely stop a network. Vampires will enhance energy usage even in situations of minimal-energy routing and when MAC protocols of power conserving are used; these attacks cannot be prohibited at MAC layer.

REFERENCES

[1] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

[2] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[3] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[4] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[5] L.B. Oliveira, D.F. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, TinyTate: Computing the Tate pairing in resource-constrained sensor nodes, NCA, 2007.

[6] Kihong Park and Heejo Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, INFOCOM, 2001.