Available online at: http://www.ijmtst.com/ncceeses2017.html

Special Issue from 2nd National Conference on Computing, Electrical, Electronics and Sustainable Energy Systems, 6th – 7th July 2017, Rajahmundry, India

A New Technique to Enhance the Wireless Sensor Network Lifetime by Mitagate Depletion Attacks

Kothapalli Alwar Sarada[1] | K.Surendra[2]

[1]PG Scholar, Department of CSE, Godavari Institute of Engineering and Technology, Rajahmundry, Andhra Pradesh, India.
[2]Associate Professor, Department of CSE, Godavari Institute of Engineering and Technology, Rajahmundry, Andhra Pradesh, India.

To Cite this Article
Kothapalli Alwar Sarada and K.Surendra, "A New Technique to Enhance the Wireless Sensor Network Lifetime by Mitagate Depletion Attacks", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 04, July 2017, pp. 71-74.

ABSTRACT

WSNs convert extra and additional vibrant to the ordinary operative of people and organizations, obtain ability liabilities develop less acceptable. Lack of accessibility can make the change between businesses as typical and lost efficiency, power outages, environmental disasters, and even lost lives; thus high accessibility of these networks is a grave property, and would hold even below malevolent conditions. We treasure that all scrutinized protocols are disposed to depletion attacks, which are disturbing, tough to detect, and are relaxed to convey out by as few as one malevolent insider transport only protocol-compliant messages.

Keywords: *routing, ad hoc networks, sensor networks, wireless networks*

I. INTRODUCTION

Depletion attacks are not procedure precise, in that they do not trust on project possessions or application liabilities of specific routing protocols, but somewhat feat general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing. Neither do these attacks trust on inundating the network with great amounts of data, but slightly attempt to communicate as little data as conceivable to realize the major liveliness channel, averting a rate restrictive explanation. Later depletion attacks use protocol-compliant messages, these spells are self-same trying to perceive and prevent. In the wickedest case, a lone depletion attacks can rise network-wide energy convention. We deliberate methods to alleviate these types of attacks, counting a new proof-of-concept protocol that provably confines the harm caused by depletion attacks throughout the packet forwarding stage.

II. RELATED WORK

Deng et al. discourse path-based DoS attacks and defenses counting using one-way hash chains to border the number of packets sent by a given node, preventive the rate at which nodes can communicate packets. While this approach may shield against traditional DoS, where the trouble maker engulfs honest nodes with large amounts of data, it does not shield against "intelligent" adversaries who usage a small number of packets or do not create packets at all.

III. LITERATURE SURVEY

We recommend a accurate outline in which safety can be exactly distinct and routing protocols for mobile ad hoc networks can be demonstrated to be protected in a severe manner. Our outline is personalized for on-demand source routing

protocols, but the universal principles are appropriate to other types of protocols too. Our method is based on the simulation standard, which has previously been used broadly for the investigation of key establishment protocols, but, to the greatest of our information, it has not been practical in the setting of ad hoc routing so far.

We highlight the reputation of well-organized caching methods to stock the least energy route material and suggest the use of an 'energy aware' link cache for storage this information. We associate the concert of an on-demand minimum energy routing protocol in terms of energy reserves with a current on demand ad hoc routing protocol through reproduction. We converse the application of Dynamic Source Routing (DSR) protocol by the Click modular router on a real life test-bed containing of laptops and wireless Ethernet cards.

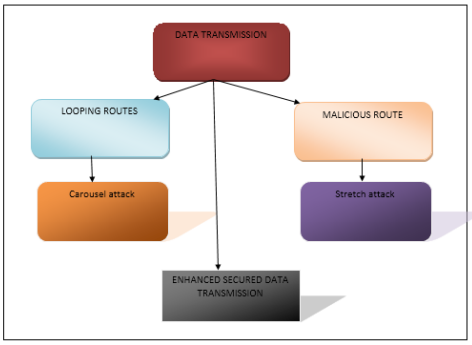
IV. PROBLEM DEFINITION

Depletion attack as the configuration and broadcast of a message that grounds additional energy to be expended by the network than if an authentic node communicated a message of equal size to the same destination, though using diverse packet headers. We extent the asset of the attack by the percentage of network energy used in the benevolent case to the energy use din the malevolent case, i.e., the ratio of network-wide power application with malicious nodes existing to energy usage with only honest nodes when the number and extent of packets referred remains persistent.

V. PROPOSED APPROACH

DoS attacks in wired networks are commonly considered by amplification. An adversary can intensify the resources it spends on the attack. Though, the development of routing a packet in any multi hop network, a source combines and transmits it to the next hop near the destination, which communicates it additional, until the destination is stretched, consuming resources not only at the source node but also at every node the message moves complete. If we contemplate the collective energy of a complete network, amplification attacks are continuously possible, given that an adversary can comprise and send messages which are treated by each node along the message track.

SYSTEM ARCHITECTURE:



VI. PROPOSED METHODOLOGY

NETWORK CREATION:

Network model with Sink, Source and with Six nodes namely Node A, B, C, D, E, F. Every node will be allocated unique Identity number. And too where topology detection is complete at transmission time, and static protocols, where topology is exposed throughout an initial setup phase, with episodic reawakening to knob rare topology changes.

CAROUSEL ATTACK:

It aims source routing protocols by developing the in adequate confirmation of message headers at forwarding nodes, letting a single packet to recurrently negotiate the same set of nodes. In first attack, an adversary composes packets with deliberately familiarized routing loops.

STRETCH ATTACK:

The stretch attack surges packet path lengths, instigating packets to be treated by a number of nodes that is sovereign of hop count along the shortest path among the adversary and packet destination. In our second attack, also aiming source routing, an adversary theories affectedly long routes, potentially negotiating every node in the network.

ENERGY LEVEL IDENTIFICATION:

A node is eternally disabled once its battery power is drained; let us momentarily consider nodes that recharge their batteries in the field, using whichever continuous charging or swapping between active and recharge cycles. In the continuous charging instance, power-draining attacks would be active only if the opponent is able to consume power at least as fast as nodes can revive.

SECURED TRANSMISSION:

The secured transmission finished in the nodes by overcoming the depletion attacks. Where the data trips in the honest route and justifying the depletion attacks occurrences.

Algorithm:

ECC ALGORITHM

Adding distinct points P and Q

If P and Q are two distinct points on an elliptic curve, and the P is not -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R.

Point Multiplication

- A point P on the elliptic curve is multiplied with the scalar K using elliptic curve equation to obtain another point Q on the same elliptic curve ie, KP=Q.
- Point multiplication is achieved by two basic elliptic curve operations point addition and doubling.
- Example
- Let P be a point on an elliptic curve.
- Let K be the scalar that is multiplied with point P to get another point Q on the curve ie, Q=KP
- IF K=23 then KP= 23. P =2(2(2(2P)+P)+P)+P.
- Thus the point multiplication uses point addition and doubling repeatedly to find the result
- The method is called " Double and add"

*Addition: If a,b € Fp, then a+b = r in Fp, where r € [0, p-1] is the remainder when the integer a+b is divided by p. This is known as addition modulo p and written a+b = r (mod p)

* Multiplication: If a,b € Fp , then a*b=s in Fp, where s € [0, p-1] is the remainder when the integer a.b is divided by p. This is known as multiplication modulo p and written a.b = s (mod p)

Elliptical curves over Finite fields

* Let Fp be a prime finite field so that p is an odd prime number, and let a,b € Fp satisfy $4a^3+27b^2+6 \neq 0$ (mod p).

* Then an elliptic curve E(Fp) over Fp defined by the parameters a,b € Fp consists of the set of solutions or points P = (x,y) for x,y € Fp to the equation $y^2 = x^3+ax+b$ (mod p)

The Elliptic Curve Discrete Logarithm Problem

- Let P and Q are the two points on an elliptic curve such that KP=Q where K is a scalar.
- Given P and Q it is computationally infeasible to obtain k, if k is sufficiently large.
- K is the descreatelogaritham of Q to the base P.

Elliptic curve domain parameters

*These are the parameters that must be agreed by both parties involved in secured and trusted communication using ECC.

- Generally the protocols implementing the ECC specify the domain parameters to be used.
- The domain parameters of ECC over F_p are T= (p,a,b,G,n,h)

* P is the prime number defined for the finite field F_p.

* a,b € F_p are the parameters specifying the elliptic curve $E(F_p)$defined by the equation $y^2 = x^3+ax+b$ (mod p)

* G is the generator point (x_G, y_G), a point on the elliptic curve chosen for cryptographic operations.

* n is the order of the elliptic curve, the scalar for point multiplication is chosen as a number between 0 and n-1.

* h is an integer defining the cofactor h = # $E(F_p)/n$ where # $E(F_p)$ is the number of points on an a elliptic curve

Generation of Elliptic curve domain parameters

*Input: The approximate security level in bits required from the elliptic curve

— This must be an integer t € {56,64,80,96,112,128,192,256}

- Generate elliptic curve domain parameters over F_p as follows

*Select a prime p such that $[\log_2 p] = 2t$ to determine the finite field F_p

*Select elements a,b € F_p to determine the elliptic curve $E(F_p)$ defined by the equation: $E : y^2 = x^3+ax+b$ (mod p) using the constraint $4a^3 + 27b^2 \neq 0$.

- A base Point G= (X_G , Y_G) on $E(F_p)$.
- A prime n which is the order of G
- h is the cofactor ($\#E(F_p)/n$) which should be ≤4.

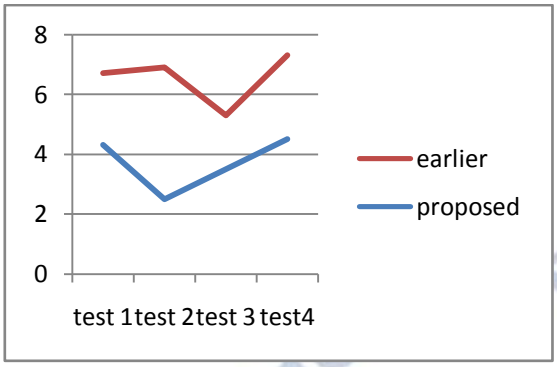
Output T=(p,a,b,G,n,h).

ECC key pairs :

- Given some elliptic curve domain parameters T = (p,a,b,G,n,h) an elliptic curve key pair (d, Q) associated with T consists of an elliptic curve private key d which is an integer in the interval [1,n-1], and an elliptic curve public key Q = (x_Q, y_Q)
- The public key is obtained by multiplying the private key with the Generator point G in the curve ie Q=dG.
- Generate an elliptic curve key pair as follows:
  - 1. Randomly select an integer d in the interval [1,n-1].
  - 2. Calculate Q = dG.

- 3. Output (d,Q).

VII. RESULTS



The Proposed ECC Algorithm shows efficiency reducing computation overhead compared to earlier technique.

EXTENSION WORK:

We encompass secure transmission by consuming an effective key management scheme for sensor networks. The planned key management scheme utilizes the fact that a sensor only communicates with a minor portion of its neighbors and accordingly condenses the communication and computation overheads of key setup.

VIII. CONCLUSION

An innovative discussion of resource consumption attacks that use routing protocols to enduringly incapacitate ad hoc wireless sensor networks by reducing nodes' battery power. These attacks do not be contingent on particular protocols or implementations, but relatively uncover vulnerabilities in a quantity of popular protocol classes. This paper discovers reserve reduction attacks at the routing protocol layer, which enduringly disable networks by speedily draining nodes' battery power. These "depletion" attacks are not explicit to some specific protocol, but relatively rely on the properties of various current classes of routing protocols.

REFERENCES

[1] The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.

[2] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[3] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[4] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[5] . Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[6] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[7] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.

[8] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.

[9] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[10] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[11] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[12] T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003. [13] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[13] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[14] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.