Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.668 – 679

RESEARCH ARTICLE

DEFENDING AGAINST VAMPIRE ATTACKS IN WIRELESS SENSOR NETWORKS

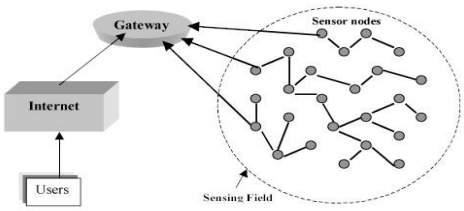
Miss. V.Subha*, **Mrs. P.Selvi**, M.Sc., M.Phil.**
*M.Phil(Computer Science), Research Scholar
Vivekanandha College for Women, Unjanai, Tiruchengode, India
******Assistant Professor in Computer Science
Vivekanandha College for Women, Unjanai, Tiruchengode, India

ABSTRACT: Wireless sensor network is a one main issue in wireless ad-hoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks require solution for conserving energy level. One new type of attack called vampire attacks, which occurring at network layer. It leads to resource depletion (energy) at each sensor nodes, by destroying battery power of any node. It transmits a small complaint messages to disable a whole network, hence it is very difficult to detect and prevent. Existing protocols are not focusing on this vampire attack happening on routing layer, hence there exist two types of attacks namely, carousel and stretch attack. Hence there is a large of energy loss. New protocol called VSP, a valuable and secure protocol is proposed along with the key management protocol to avoid this vampire attack. By using this, existing problems can be overcome. The existing system does not offer a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. The system proposed defenses against some of the forwarding-phase attacks and described VSP, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The proposed system introduces a novel authentication and key management mechanism called Hybrid Key Management. It is robust and scalable under limited memory constraints. It ensures strong security guarantees by using Low Power Routing (RPL).The proposed system avoids vampire attack by Elliptic curve Diffie-Hellman algorithm for authentication and Modified RSA algorithm for data Encryption.

Keywords – wireless sensor networks, vampire attack, resource consumption, encryption, decryption, security

1. INTRODUCTION

Sensor network is composed of a large number of sensor nodes that are deployed in a wide area with very low powered sensor nodes. The wireless sensor networks can be utilized in a various information and telecommunications applications. The sensor nodes are very small devices with wireless communication capability, which can collect information about sound, light, motion, temperature etc and processed different sensed information and transfers it to the other nodes.



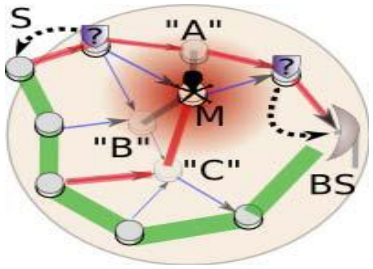
Wireless Sensor Network

2. LITERATURE SURVEY

Gergely Acs, Levente Buttyan, And Istvan Vajda (2005). Our approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but to the best of our knowledge, it has not been applied in the context of ad hoc routing so far also propose a new on-demand source routing protocol, called endair and demonstrate the usage of our framework by proving that it is secure in our model. *Jing Deng, Richard Han, Shiva Kant Mishr (2005).* The system has proposed a novel and robust set of mechanisms to maintain one -way hash chains given packet loss and topology changes. The implementations show that the scheme is feasible in current sensor network platforms, and incurs modest overhead the OHC -based mechanism is applicable not just to unicast paths, but also can be extended to counteract PDoS attacks against a reliable end-to-end connection and multipath routing in WSNs. *Tuomas Aura, Pekka Nikander, Jussipekka Leiwo (2002).* Denial of service by server resource exhaustion has become a major security threat in open communications networks. Public-key authentication does not completely protect against the attacks because the authentication protocols often leave ways for an unauthenticated client to consume a server's memory space and computational resources by initiating a large number of protocol runs and inducing the server to perform expensive cryptographic computations show how stateless authentication.

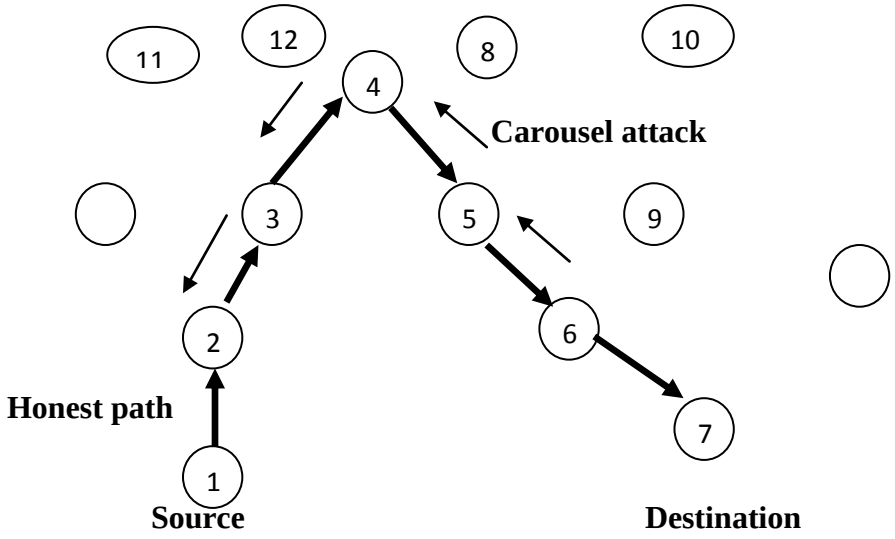
3. PROBLEM DESCRIPTION
VAMPIRE ATTACK

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. The vampire attacks can be classified has two types. There are: one is Carousel attack and other is Stretch attack.



3.1CAROUSEL ATTACK

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. In this malicious node introduces loop in the path of packet travel purposely to drain the energy of honest nodes. An example of this type of route is in Fig 3.1 the thick path shows the honest path and thin shows the malicious path.

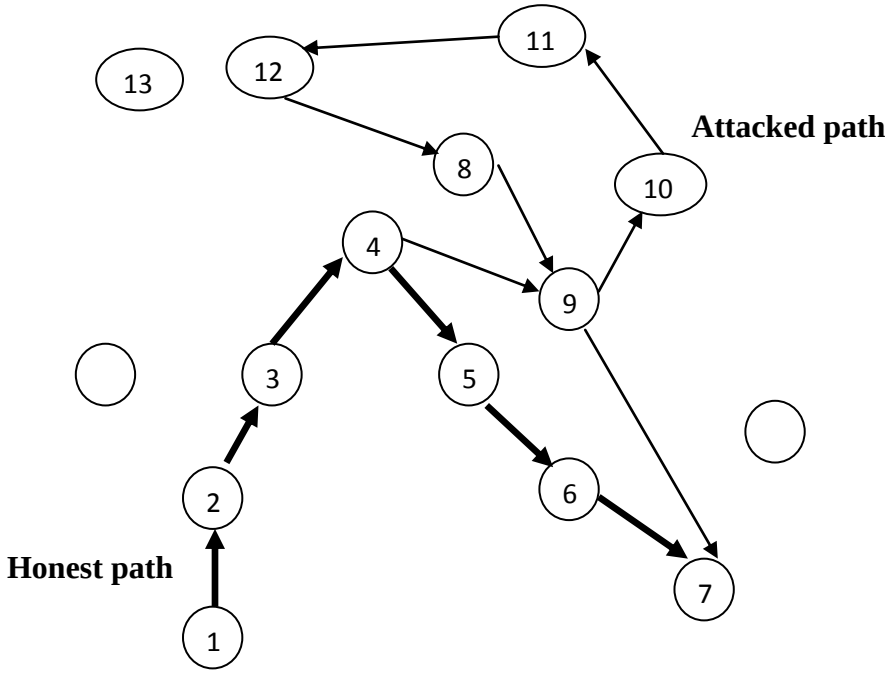


The Carousel attack same node appears in the route many times.

3.2 STRETCH ATTACK

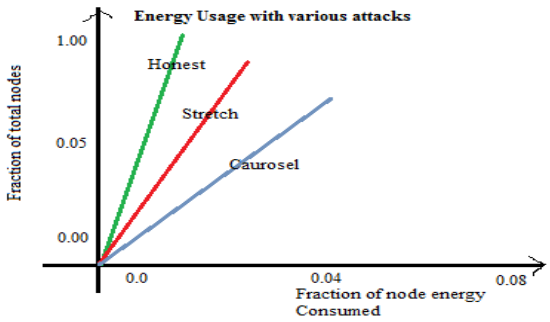
Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. Below the figure honest path shown with thick lines and adversary or malicious path with thin

lines. The honest path is very less distant but the malicious path is very long to make more energy consumption.



Stretch Attack With Two Different Paths From Source To Destination. (4-9-10-11-12-8-9—long route).

As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected with some losing almost 10 percent of their total energy reserve per message.



Node Energy Distribution Under Various Attack Scenarios.

Vampire attack happens in the network in the sense, any of the nodes in the network which is affected or infected and this nodes behavior is abruptly changing for the network behavior, this kind of nodes are called "Malicious node". If malicious nodes present in the network energy that have been using by each and every nodes will increases drastically. The malicious node has been place in the network uniquely. First In between the routing nodes, and the second placed in the Source node itself. The chance of placing a malicious node in the routing path this makes causing damage in network. This Dissertation is mainly concentrates on the identification and avoidance of the malicious node.

SYSTEM OBJECTIVE

- Protect from the vampire attacks.
- Secure level is high.
- Boost up the Battery power.
- Guarantee loop freeness.
- Avoid packet loss

4. METHODOLOGY

Vampire attacks are most popular attack in networks. To overcome this attack base station sends a common key to all the node and the node send a reply along with public key to base station. Suppose, an attacker node is appeared and try to communicate in the network. An attacker node also sends the beacon request with the public key for communication. Base station verifies the public key and it identifies that it is not in the sequence of valid public key, So that Base station simply reject the malicious node. In this way secured communication is established and communication to perform successfully.

VALUABLE SECURE PROTCOL

Valuable secure protocol do the functionality such as authentication and Encryption , Decryption to secure vampire attack.

4.1 ELLIPTIC CURVE DIFFIE – HELLMAN

ECDH key exchange is the elliptic curve analogue of the classical Diffie-Hellman key exchange, the ECDH can be used to establish a shared secret key between two entities using an insecure communication channel. The ECDH algorithm is used for authentication and to identify

the Malicious node .Once malicious node is identify to information is transfer to the destination to avoiding the carousal and stretch to preserve the energy. Elliptic Curve Diffie-Hellman Key Exchange Algorithm is used to quicken the key verification process based on coordination between the sensor nodes. A user requests its neighboring sensor nodes for broadcast services after registering and obtaining the security certificates. The sensor nodes perform a mutual authentication process that authorizes the WSN access only to an authenticated user. The user needs to sign the command/query before transmitting it to the sensor nodes. The user signs a command or query and forwards it to the various sensor nodes

The two communicating parties, usually called A and B, have to perform in order to obtain a shared secret we assume that A and B use the same set of domain parameters D= (p,a,b,G,n,h). Also, each party must have a key pair suitable for elliptic curve cryptography, consisting of a private key d(a randomly selected integer in the interval [1,n-1]), where n is the order of the curve and a public key Q = d*G (G is the generator point)

A key pair be (d_A,Q_A)

B key pair be (d_B,Q_B)

Each party must have the other party's public key (an exchange must occur).

A computes $(x_a,y_a) = d_A*Q_A$

B computes $(x_b,y_b) = d_B*Q_B$.

The end A Computes KA= (X_a, Y_a) = dA * QB

The end B Computes KB= (X_b, Y_b) = dB * QA

The shared secret calculated by both parties is equal, because

$$d_A*Q_B = d_A,d_BG = d_Bd_AG = d_B*Q_A$$

The only information about her private key that Alice initially exposes is her public key. So, no party other than A can determine A private key, unless that party can solve the elliptic curve discrete logarithm problem. B private key is similarly secure. No party other than A or B can compute the shared secret, unless that party can solve the elliptic curve Diffie–Hellman problem.

4.2 MODIFIED – RSA ALGORITHM

To secure data or information by a modified RSA cryptosystem based on 'n' prime. This is a new technique to provide maxi mum security for data over the network. It is involved encryption and decryption. Prime number used in a modified RSA cryptosystem to provide security over the networks .In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. We used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provide security.

PROCEDURE

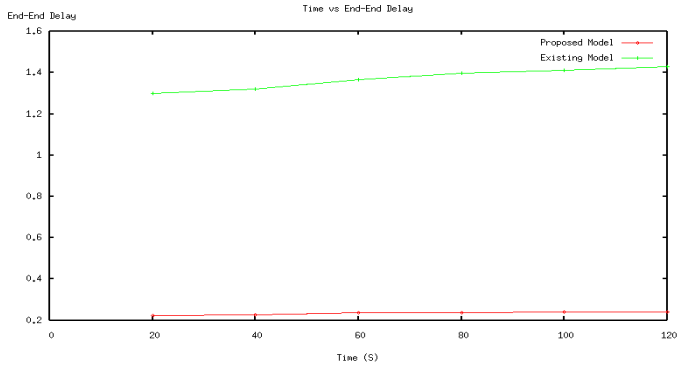
1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (phi) φ = (p-1)(q-1).
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi). The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d. Other times we might write the key pair as ((N, e), d).]

- n is known as the modulus.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.
- Encryption rule: ciphertext, c = RsaPublic(m) = m^e mod n, 1 < m < n-1
  Decryption rule: plaintext, m = RsaPrivate(c) = c^d mod n
  Inverse transformation: m = RsaPrivate(RsaPublic(m))
-

5. EXPERIMENTS AND RESULTS

Energy consumption are evaluated and it is compared with the Existing system. Security enhancements in the proposed system is also evaluated. Packet forwarding overhead, path diversity than BVR. Since the forwarding phase should last considerably longer than setup, PLGP offers performance comparable to BVR in the average case. It includes path attestations,

increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification requirements for intermediate nodes also increases processor utilization, requiring time and additional power. Of course there is nothing to be gained in completely non-adversarial environments, but in the presence of even a small number of malicious nodes, the increased overhead becomes worthwhile when considering the potential damage of Vampire attacks. By using the Modified RSA algorithm in the Cooperative Wireless Sensor Network we increase the performance of the parameters in the network. The Parameters are security, accuracy, tolerance, packet delivery ratio, energy efficiency, delay parameters, energy models and throughput.



Time vs End Delay

From the above graph, it shows end to end delay is low in proposed system when compared to the existing system. Proposed systems minimize the delay and maximizing the lifetime of event-driven wireless sensor networks. i.e. network lifetime, subject to a constrain on the expected end- to-end packet-delivery delay.

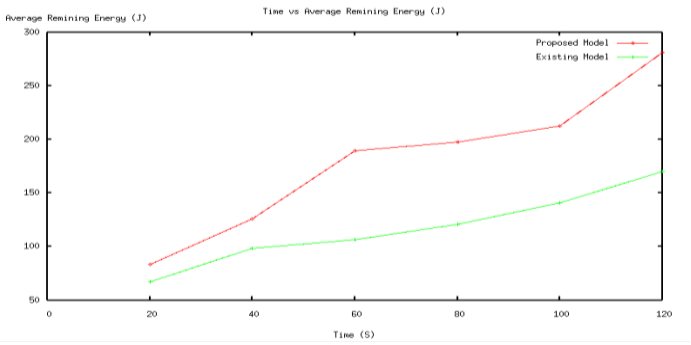
End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

- $d_{end\text{-}end} = N[\ d_{trans} + d_{prop} + d_{proc}]$

  $d_{end\text{-}end}$= end-to-end delay
- d_{trans}= transmission delay
- d_{prop}= propagation delay
- d_{proc}= processing delay
- d_{queue}= Queuing delay
- N= number of links (Number of routers + 1).

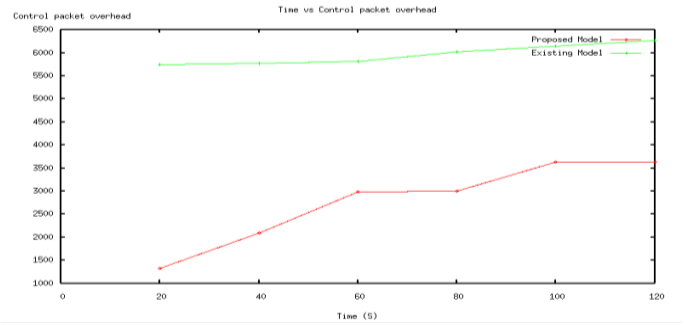
Each router will have its own dtrans, dprop, dproc hence this formula gives a rough estimate. The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections



Time vs Average Remaining Energy.

From the above graph, it shows the energy saving process is higher in proposed system than existing system. Due to less energy consumption proposed system increases the network life time.

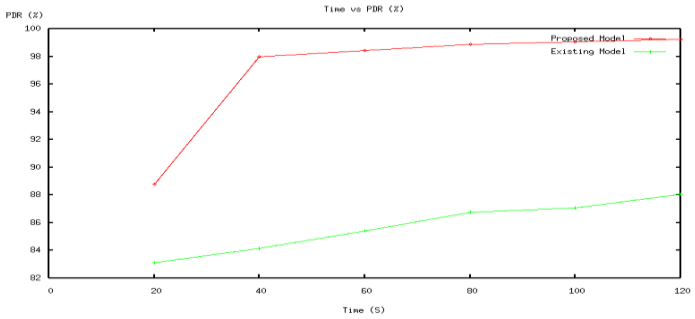


Time vs Control packet overhead.

From the above graph, it represent the packet loss process comparing with the existing system. The lower value of end to end delay means the better performance of the protocol.

- Packet Lost : the total number of packets dropped during the simulation.
- Packet lost = Number of packet send – Number of packet received.

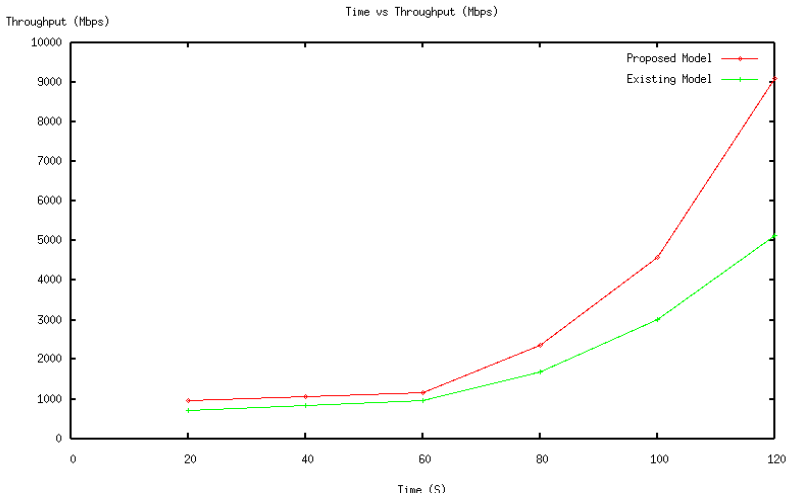
The lower value of the packet lost means the better performance of the protocol.



Time vs PDR

From the above graph, it represent the packet delivery report. Where proposed system increase the packet delivery ratio than the existing one. The greater value of packet delivery ratio means the better performance of the protocol. The **ratio** of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. **Packet delivery ratio**: the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send



Time vs Throughput.

From the above graph, it represents the data rate. In proposed System, Data rate is higher than the Existing system. The data transfer rate is commonly used to measure how fast data is transferred from one location to another.

6. CONCLUSION AND FUTURE SCOPE

A new class of resource consumption attacks that are routing protocols to permanently disable ad hoc wireless sensor networks by depleting node battery power. This attack is mitigated by proposing a Valuable secure protocol using Hybrid key Management scheme and vulnerabilities exposed in existing protocol are evaluated. Elliptic Curve Diffie-Hellman which is more lightweight compared to regular Diffie-Hellman. This approach includes group key establishment for authentication and connecting the network. By using a distributed architecture the load of key management is reduced. Second the scheme deploys the Modified RSA algorithm for encryption /decryption during data transmission. Specifically, the scheme can be extended to hybrid architecture to provide better scalability. Consequently, the extended scheme is both fault-tolerant and efficient in terms of integrity and confidentiality. The simulation result show that the impact on the system was reduced to great extended after implementing in the algorithm. A full solution is not given yet but some amount of damage was avoided. The proposed technique routing protocol are provably bounds damage from Vampire attacks by verifying that packets consistently make a progress toward their destinations and reduce the reimbursement. The cryptographic primitives and key management for giving the security in a network against Vampire attack. In future the process will be extended and concentrates on security in routing by implenments another one new technique and improve the energy efficiency of the system by considering residual energy and implement energy aware network to increase the life time of the system.

REFERENCES

1. Shih-Lin Wu,Yu –Chee Tseng **"*WIRELESS AD HOC NETWORKING*"** Auerbach Publications , and ISBN :10: 0-8493-9254-3,Special Indian Edition.

2. Kazem Sohraby, Daniel Minoli, Taieb Znati "***WIRELESS SENSOR NETWORKS*: *TECHNOLOGY, PROTOCOLS AND APPLICATIONS*"** Wiley Publications(21 July 2010), and ISBN : 10: 8126527307.

3. Jagannathan Sarangapani "***WIRELESS AD HOC AND SENSOR NETWORKS PROTOCOLS, PERFORMANCE AND CONTROL*"** Taylor & Francis Group Published In: 2007, and ISBN10:0824726758 .

4. Waltene gus Dargie, Christian oellabauer "***FUNDAMENTALS OF WIRELESS SENSOR NETWORK: THEORY AND PRACTICE*****"** Wiley publications and ISBN : **0-8493-8227-0**.

5. Mohammad llyas,Imad fahgoub "***HAND BOOK OF SENSOR NETWORKS COMPACT WIRELESS AND WIRED SENSING SYSTEMS*****"** Taylor & Francis Group Published In:2006 and ISBN 0-203-53926.

6. Feng zhao,Leonidas *"**WIRELESS SENSOR NETWORK : AN INFORMATION PROCESSING APPROACH"*** Wiley Publications(21 July 2010), and ISBN :**0-4200-80387-0**.

