International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Shared Key Based Jamming Mitigation in Wireless Network using Diffie Hellman Elliptic Curve Cryptography

S. Rajeswari[1], Dr V. Anuratha[2]

[1]Assistant Professor, PG Department of Computer Application, Sree Saraswati Thiyagaraja College, Pollachi- 64207

[2]Assistant Professor, Head, PG Department of Computer Science, Sree Saraswati Thiyagaraja College, Pollachi- 64207

Abstract: ***Wireless sensor networks (WSNs) are increasingly used as an enabling technology in a variety of domains.This paper focused to remove the jamming attacks using shared key based approch in wireless network. Existing systems such as DOS resistant authentication, RFID systems can be applied to remove the jamming attack in the multi path routing and the routing protocols are not permanently disable in the ad hoc wireless network by depending node battery power .In this paper it is proposed to avoid the jamming attack using Shared Key Based Jamming Mitigation, the multi paths routings are combined and the routing protocols are permanently disable, the data loss can be more reduced compare the existing system.***

Keywords: Jamming Mitigation, Wireless Network, DHECC key , Shared Key Based Jamming Mitigation

1. Introduction

Wireless ad-hoc Sensor Networks provide one of the missing connections between the Internet and the physical world. One of the main problems in sensor networks is the limited power of nodes. Wireless ad hoc sensor networks do not require any predefined infrastructure like access points, base stations etc. for communication purposes..Vampire attacks are the most common resource depletion attacks where the energy consumed by the network to compose and transmit a message is greater when compared to that of an ordinary network[1]. Vampire attacks disrupt the working of a network immediately rather than work overtime to entirely disable a network These types of attacks not directly link with the protocols; it links with the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. The vampire attack in the WSN is not easy to discover and to predict[2] .Due to the solitary vampire attack in the networks, total force goes down and leads to the complete systems to the collapse.. In order to overcome the above attacks, an efficient intrusion detection system based on energy of nodes.

2. Literature Survey

In DOS resistant Authentication with client puzzles , the more accurate scale achieved by combine several puzzle with varying size, it protects serer that authentication , clients against resource exhaustion. But the server suspects under an attack and capacity becomes large.[4]. Using the Defending against path based DOS attacks, to overcome this problem the multipath routing improve robustness and reliability of data communication but the problem is some data can lose[5].

To improve the multipath for better protection against DOS using intrusion tolerant routing for MANET but it add physical security risk of

individual sensor nodes fall into wrong hands[11]. The multipath occurs many jamming attacks so the data have some risks. The strong cryptographic authentication for RFID systems using AES algorithm but it have very time consuming and costly[9].

3. Jamming Mitigation in Wireless network

The concept of mitigation in wireless network using the following process. First, the number of nodes can be generated in the network formation. Next the shared key can be generated in both the sender and receiver. The data can be received only when the shared key can be matched in both the sender and receiver. The nodes can be attacked by vampire attack and these nodes cannot be reach the data correctly. Finally the attacked nodes can be recovered using DHECC key the data or packets can be send by multipath. The following process can be used to recover the attacked nodes to receive the data fast. The shared key based accuracy and security jamming mitigation in wireless network contains the following process. They are Node selection , Key creation for authentication, Encryption/decryption data, Jamming avoidance,Route maintenance, Performance Evaluation.

Node selection
The node selection is new network formation; the node can be selected one as source and other as destination and other node are as created or form.

Key creation for authentication
For authentication is the shared key can be generated both in sender and receiver the key can be stored in destination node, which can be send by sender node. The authentication key is same for sender node and receiver node then the data can be received or otherwise refer the authentication key .

Encryption/ decryption of Data
The data can be encrypt in the sender node and data can be decrypt in the receive node properly. The data share the wireless network.

Route maintenance
The No. of node should be occupy between the sender and receiver node. The routes can be maintain to identify the jamming node between two nodes

Jamming Avoidance
After identifying the jamming nodes between the sender and receiver node can be removed nodes due to jamming, the data cannot be reached commend and data can be lose for this problem; the jamming node are removed from source to destination the data or message can be send and received.

Performance Evaluation
The remove the all jamming node and proper way find then delivery the data without loss and securely and more power energy saved.

3.1 System Architecture

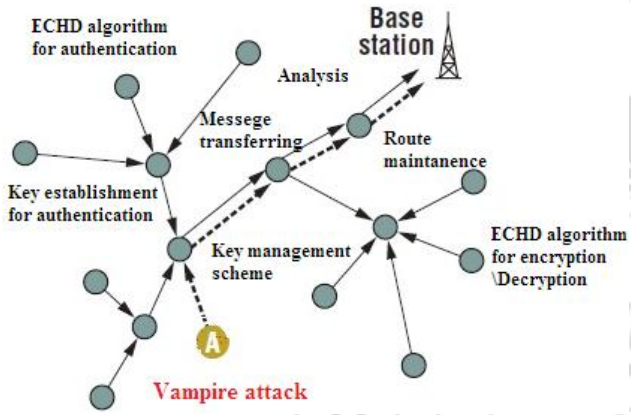


Figure 1: System Structure

4. Diffie-Hellman Key Exchange Using Elliptic Curve(DHECC)

Two levels Encryption Decryption by Diffie – Hellman key exchange method is used for a smaller and a very faster public key cryptosystem, at the same time the approach should be practical and very secure, even for the most constrained environments.

In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible. Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole.

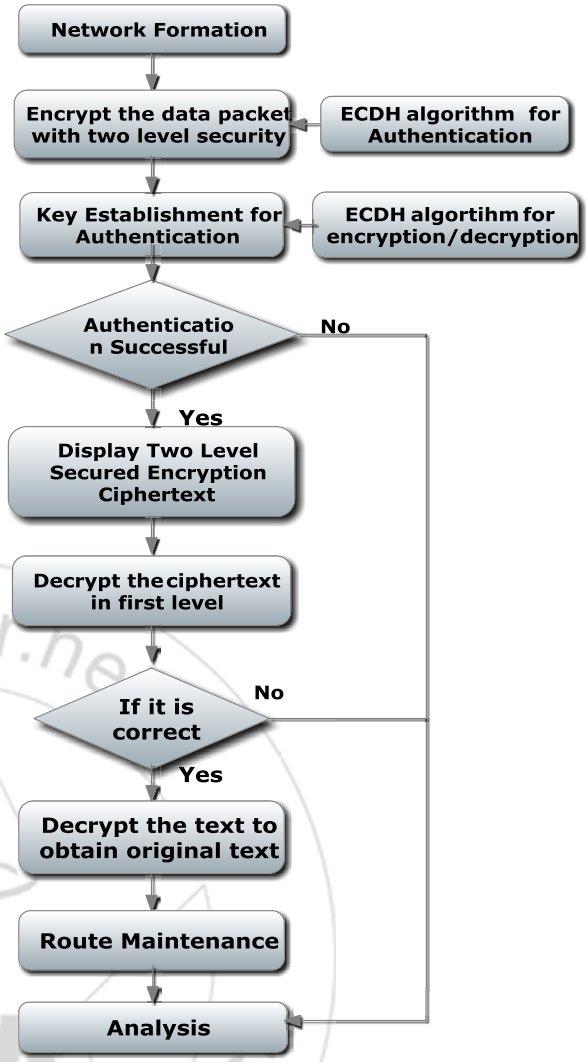


Figure 2: System Flow Chat

5. Algorithm

Function forward_packet(p)
s ← extract_source_address(p);
c ← closest_next_node(s);
if is_neighbor(c) then forward(p, c);
else
r ← next_hop_to_non_neighbor(c);
forward(p, r);
Function secure_forward_packet(p)
s ← extract_source_address(p);
a ← extract_attestation(p);
if (not verify_source_sig(p)) or
(empty(a) and not is_neighbor(s)) or
(not saowf_verify(a)) then
return ; /* drop(p) */
foreach node in a do
prevnode ← node;
if (not are_neighbors(node, prevnode)) or
(not making_progress(prevnode, node)) then
return ; /* drop(p) */
c ← closest_next_node(s);
p′ ← saowf_append(p);
if is_neighbor(c) then forward(p′, c);
else forward(p′, next_hop_to_non_neighbor(c));

6. Implementation

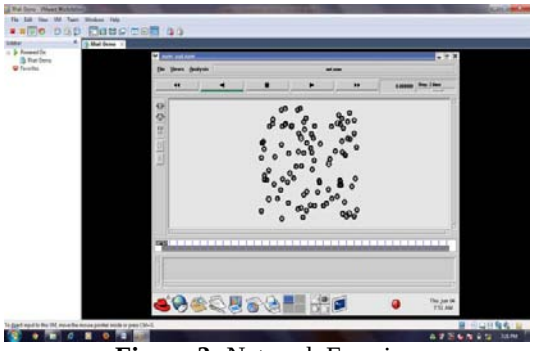


Figure 3: Network Forming

In this screen more than 100 nodes can be created in the network formation.

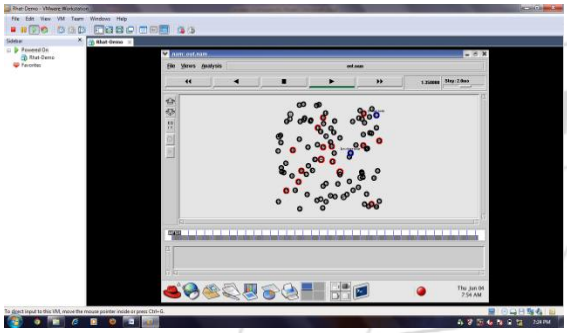


Figure 4: Jamming node in the network

In this screen the nodes can be selected as source and destination. The intermediate nodes between the source and the destination some nodes can be attacked by vampire attacks. Due to this type of attack the data can be loss from sender to receiver.

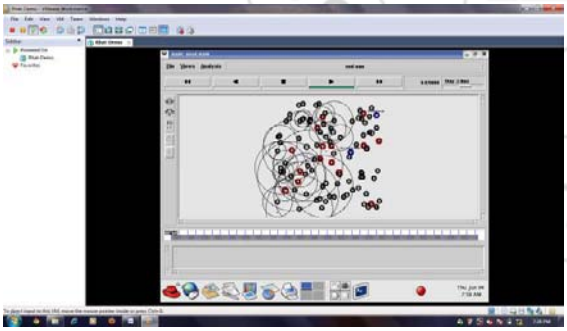


Figure 5: Network Jamming

In this process the different nodes can be transmitted in the same network path the jamming can be attacked in the nodes

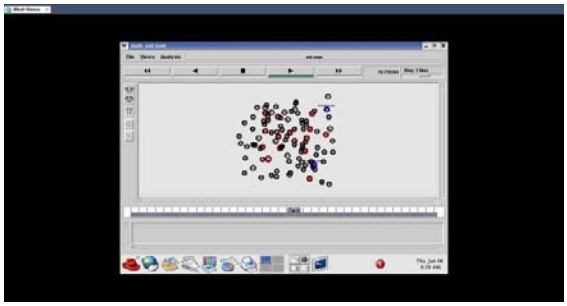


Figure 6: Node to node packet data sends

In this process select the key authentication the data packets can be send from the sender to receiver.

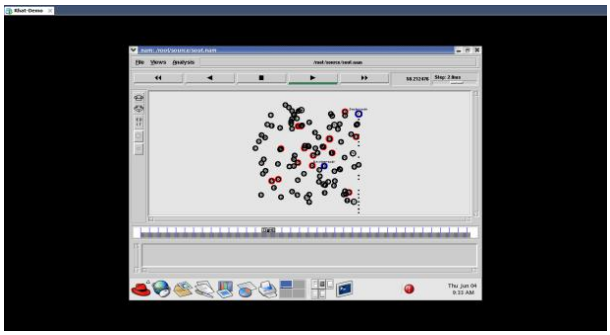


Figure 7: Shared key based Data Send to Destination

In the above process the shared key can be send to the receiver the data can be received only when the shared key matches to source and destination.

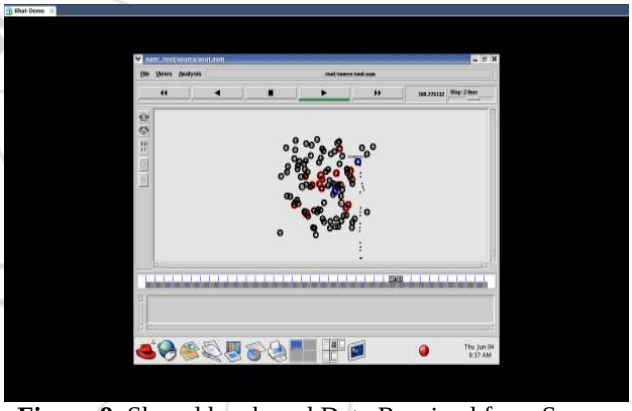


Figure 8: Shared key based Data Received from Source

In this process the shared key can be received from source and destination.

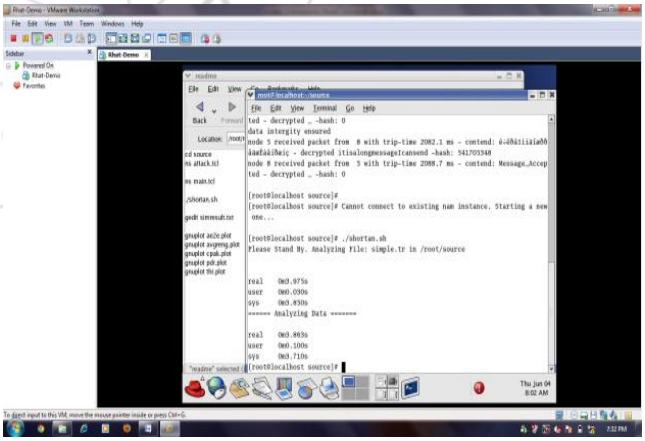


Figure 9: Network Analysis file and Data

In this process the network analysis file and data are generated.

Table 1: Simulation Result

Simulator	NS2
Simulation Area	1000m X 1000m
Numbers of Node	100
Total Remained Energy	0
Average Remained energy	0
Energy Difference	0
Packet Delivery Ratio	33.484199
Average End-end Delay	2.3432511
Average Number of Hops	2.90586259
Control Packet Overhead	579
Throughput(Mbps)	19172.4617190
Data Packet Send	37340
Data Packet Received	12503
Simulation End Time	149.990650
Total Delivery time	29061.0369431449
Total Numbers of Hops	36332
Dropped Reply Message	1
Max Number of Hops	5
Min number of hops	1

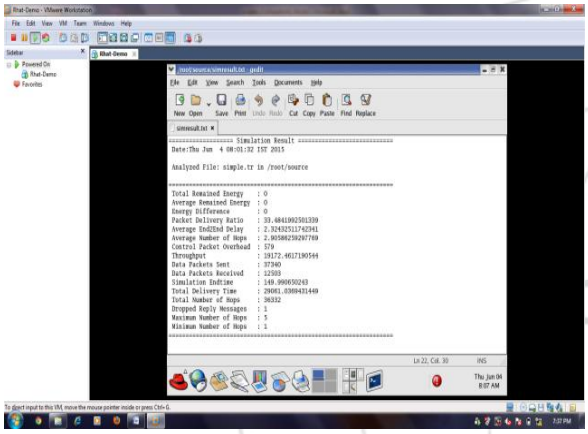


Figure 10: Simulation result

In the above process the simulation result can be generated.

Table 2: Time and Delay Comparison Chart

RFID	Delay	1.3	1.32	1.34	1.36	1.38	1.4
	Time(s)	20	40	60	80	100	120
SKBJM	Delay	0.2	0.2	0.2	0.2	0.2	0.2
	Time(s)	20	40	60	80	100	120

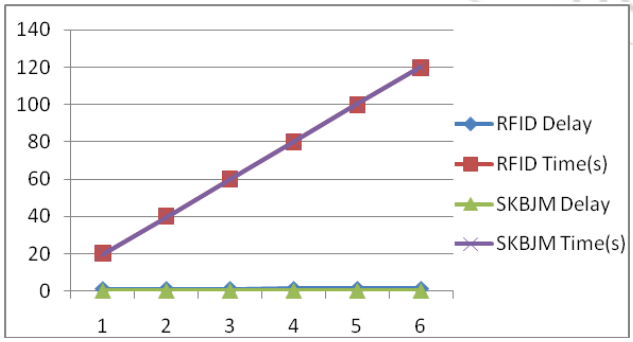


Figure 11: Time and delay comparison chart

In this chart the time and delay of network can be compared.
RFID->Radio Frequent IDentification (Existing Model)
SKBJM->Shared Key Based Jamming Mitigation**(Proposed Model)**

Table 3: Time and average remain energy

RFID	Time Avg Remain Engy	50	75	100	110	130	150
	Time(s)	20	40	60	80	100	120
SKBJM	Time Avg Remain Engy	50	120	160	175	200	250
	Time(s)	20	40	60	80	100	120

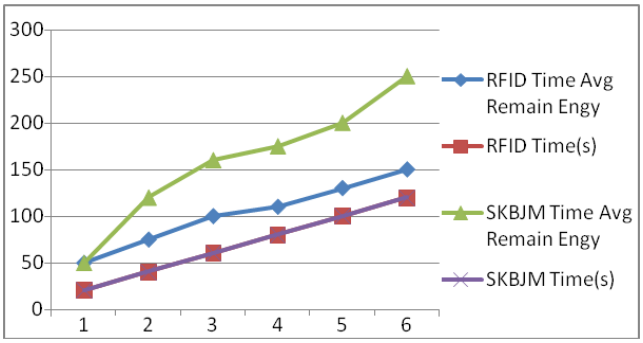
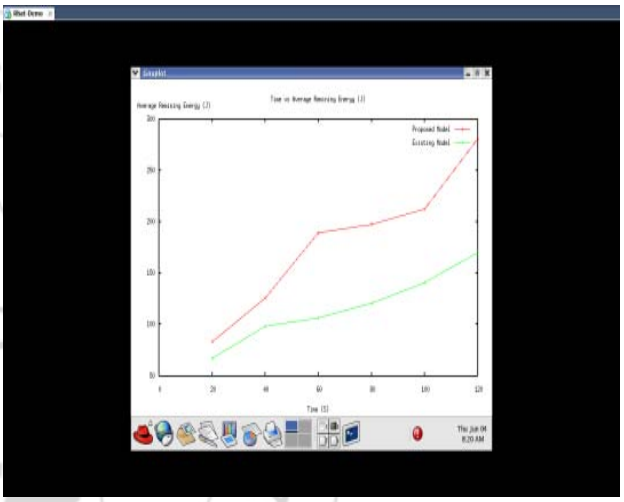


Figure 12: Time and average remain energy



Remain energy can be plotted in the graph using the proposed system

Table 4: Control Packet Overhead

RFID	PDR	82.2	82.3	82.8	83.5	85.3	86
	Time(s)	20	40	60	80	100	120
SKBJM	PDR	88	98	98.3	98.5	98.8	99.9
	Time(s)	20	40	60	80	100	120

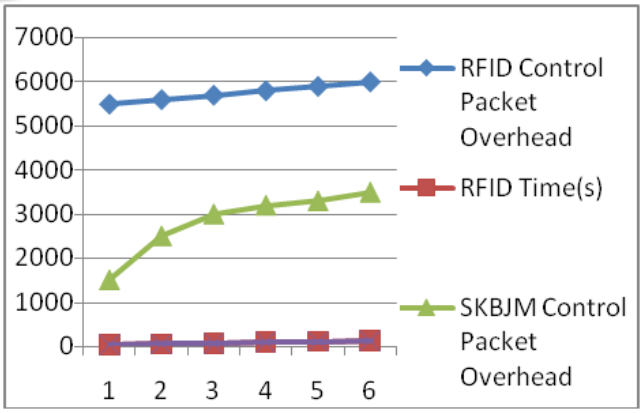
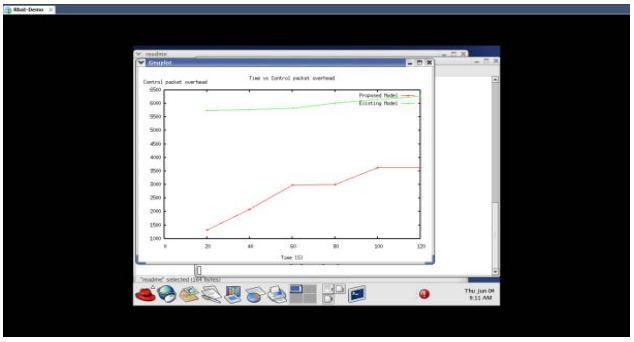


Figure 13: Control packet overhead



In the above chart the overhead packet can be controlled in our proposed system.

Table 5: Packet Datagram Ratio

RFID	CP O	5500	5600	5700	5800	5900	6000
	Time(s)	20	40	60	80	100	120
SKBJM	CPO	1500	2500	3000	3200	3300	3500
	Time(s)	20	40	60	80	100	120

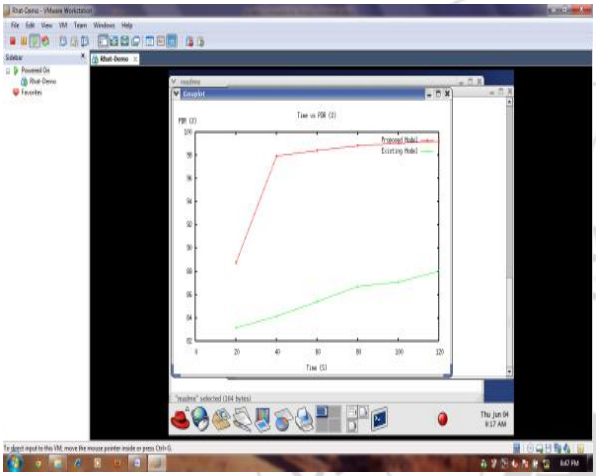


Figure 14: Packet datagram ratio

In this chart the packet datagram ratio can be plotted and compared to the existing system

Table 6: Throughput (mbps)

	Throughput (Mbps)	800	850	900	1500	2000	2500
RFID	Time(s)	20	40	60	80	100	120
SKBJM	Throughput (Mbps)	1000	2000	3000	6000	8000	9000
	Time(s)	20	40	60	80	100	120

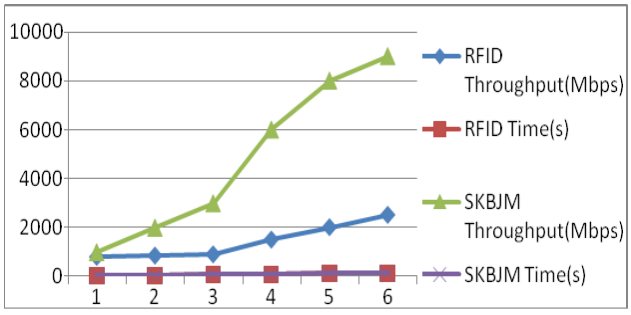
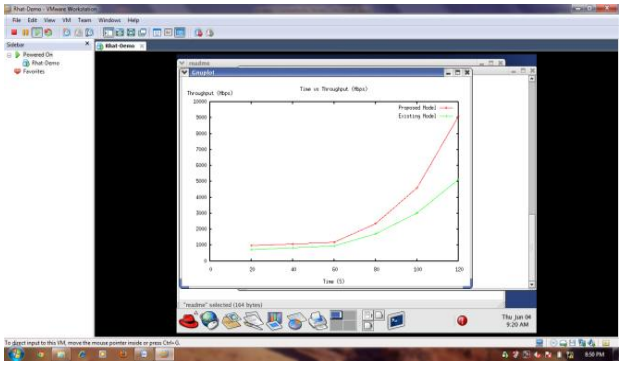


Figure 15: Throughputs



In this chart the throughputs of process can be generated and compared to an existing.

7. Conclusion

A new class of resource consumption attacks (vampire) that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power. This attack is mitigated by proposing a key management protocol, Elliptic Diffie-Hellman key exchange protocol.

In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible. Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost. By reducing hop count energy conservation can be avoided.

References

[1] The network simulator — ns-http://www.isi.edu/nsnam/ns/.
[2] http://www.isi.edu/nsnam/ns/.[2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial ofservice resilience in ad hoc networks, MobiCom, 2004.
[3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.
[5] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: realvulnerabilities and practical solutions, USENIX security, 2003.
[6] Daniel Bernstein and Peter Schwabe, New AES software speed records,INDOCRYPT, 2008.
[7] Daniel J. Bernstein, Syn cookies, 1996.

http://cr.yp.to/syncookies.html.
[8] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography,Vol. 265, Cambridge University Press, 1999.
[9] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementationsof AES on various platforms, 2009.
[10] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks,Computer 36 (2003), no. 10.
[11] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing inwireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.
[12] Thomas H. Clausen and Philippe Jacquet, Optimized linkstateroutingprotocol(OLSR),2013