



INVASION DISCOVERY AND PREVENTION TECHNIQUE FOR VAMPIRE ATTACK

M. ANITHA

st119159

EXAMINATION COMMITTEE

Dr. Teerapat Sanguankotchakorn (Chairperson)

Dr. Attaphongse Taparugssanagorn

Dr. Poompat Saengudomlert

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES
ASIAN INSTITUTE OF TECHNOLOGY

Thailand
March, 2019



Introduction

Wireless Ad hoc Sensor Networks

Spatial distribution of autonomous sensors to monitor environmental conditions such as temperature, pressure, etc., is called a **wireless sensor network**.

A set of networks where all devices are treated equally with a certain status and can also associate with similar nodes easily in a very short interval are referred to be an Ad-hoc sensor network.

Applications:

- Instantly deployable communication for military and first responders.
- Monitor environmental conditions , factory performance and troop deployment.
- Ubiquitous on demand computing power.



Vampire Attack

Definition:

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.

Features:

- Vampire attacks are not protocol specific
- They don't disrupt immediate availability
- Vampires use protocol compliant messages
- Transmit little data with largest energy drain
- Vampires do not disrupt or alter discovered paths

Objectives:

- Propose an Invasion Discovery Technique to segregate the vampire nodes from the genuine nodes in a mobile ad-hoc network.
- Reshape an existing routing protocol to resist the battery depletion attack.
- Compare the existing and proposed system using performance evaluation metrics such as throughput, packet delivery ratio and end-to-end delay.



Types of Vampire Attacks:

- ❖ Attack on stateless protocols
- ❖ Attack on stateful protocols

Stateless Protocols:

- ★ Same as source routing protocol
- ★ Source node specifies entire route to destination within packet header.
- ★ Intermediaries don't make independent forwarding decisions.

Stateful Protocols:

- ★ Nodes are aware of their topology, state, forwarding decisions.
- ★ Nodes make local forwarding decisions on that stored state.

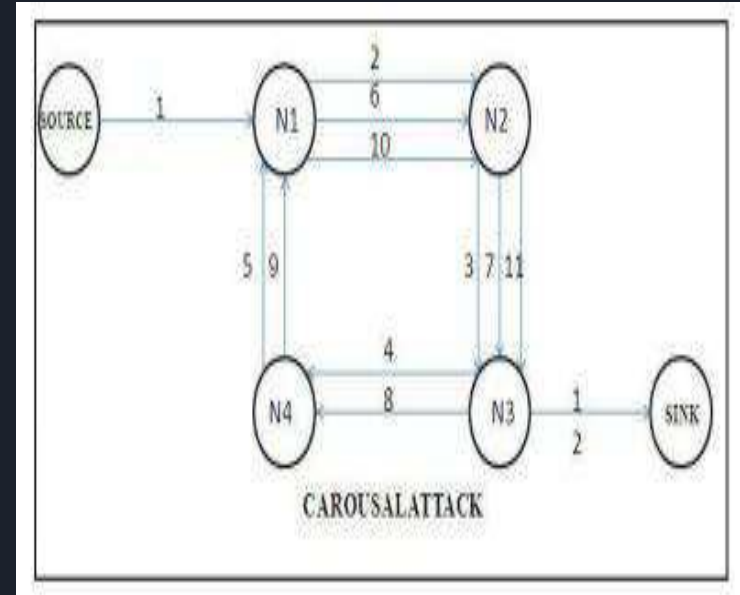
Attacks on Stateless Protocols

Types of Attacks:

- ★ Carousel attack
- ★ Stretch attack

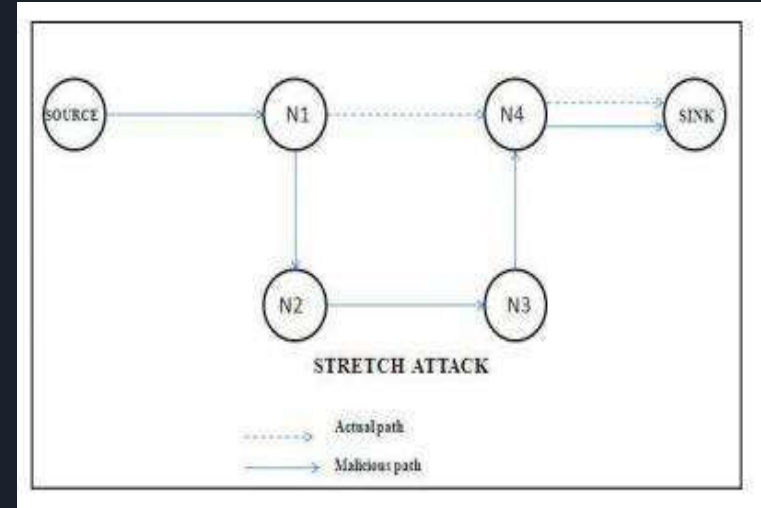
Carousel Attack:

- ❑ Adversary sends packets with routes composed of a series of loops.
- ❑ Exploits limited verification of message headers at forwarding nodes.
- ❑ Used to increase the route length beyond no of nodes in network.
- ❑ Theoretical limit: energy usage increase by a factor of $O(\lambda)$, where λ is the maximum route length.



Stretch Attack

- Adversary constructs artificially long routes traversing every node in the network.
- Causes packets to traverse larger than optimal no of nodes.
- Causes nodes that doesn't lie on optimal path to process packets.
- Theoretical limit: energy usage increase of factor $O(\min(N, \lambda))$, where N is the number of nodes in the network and λ is the maximum path length allowed.



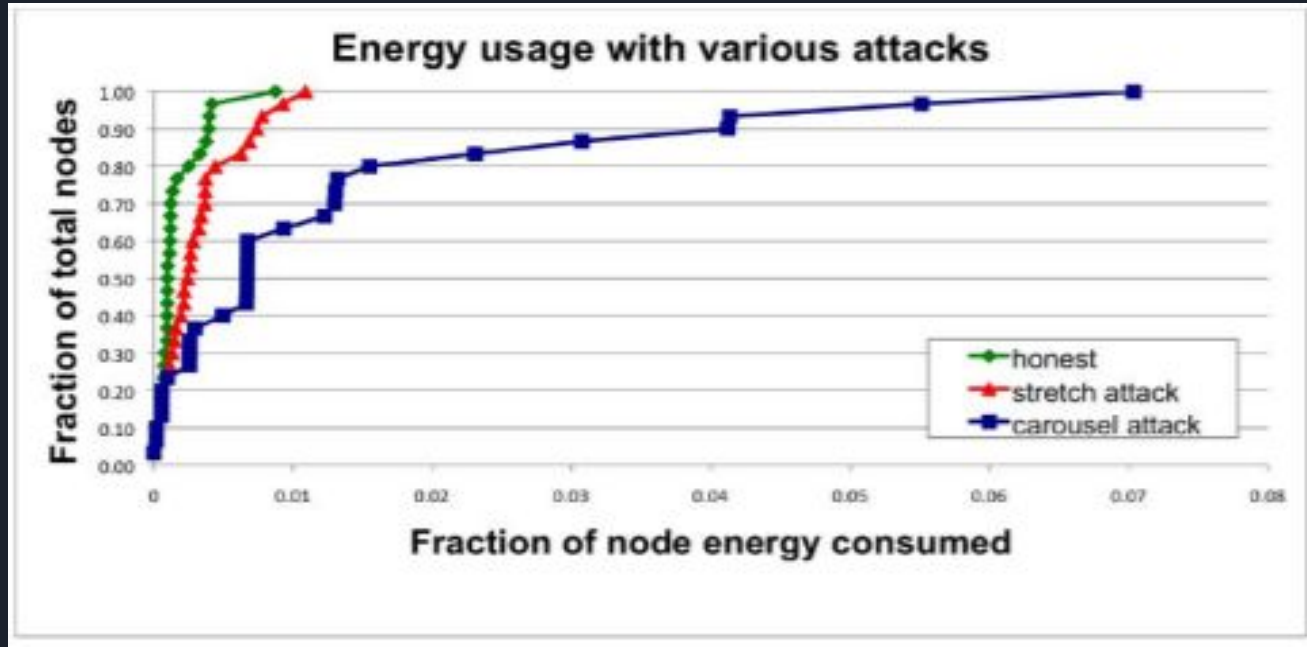


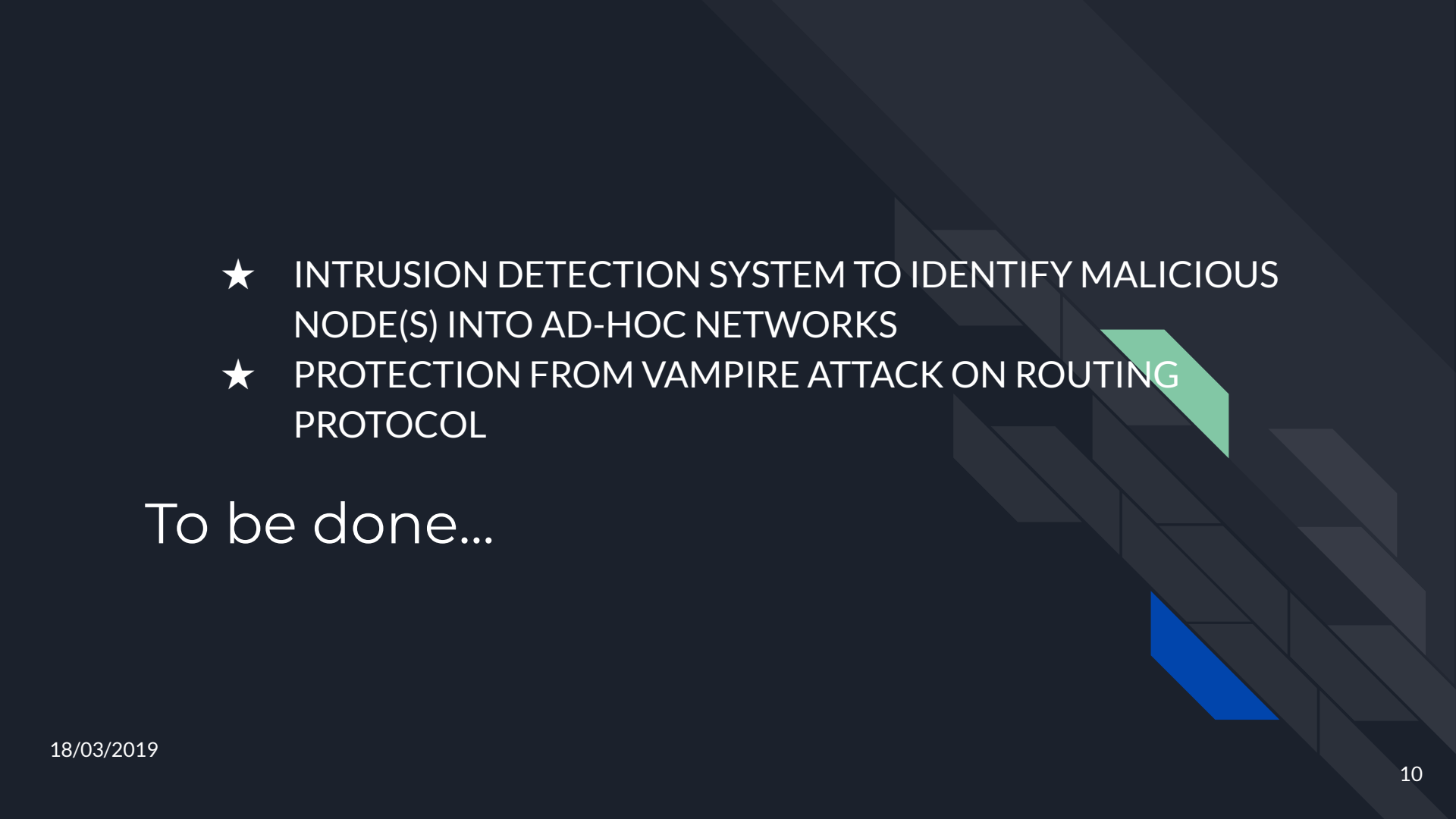
Fig: Node energy distribution under various attack scenarios. The network is composed of 30 nodes and a single randomly positioned Vampire. Results shown are based on a single packet sent by the attacker.



Software Requirement

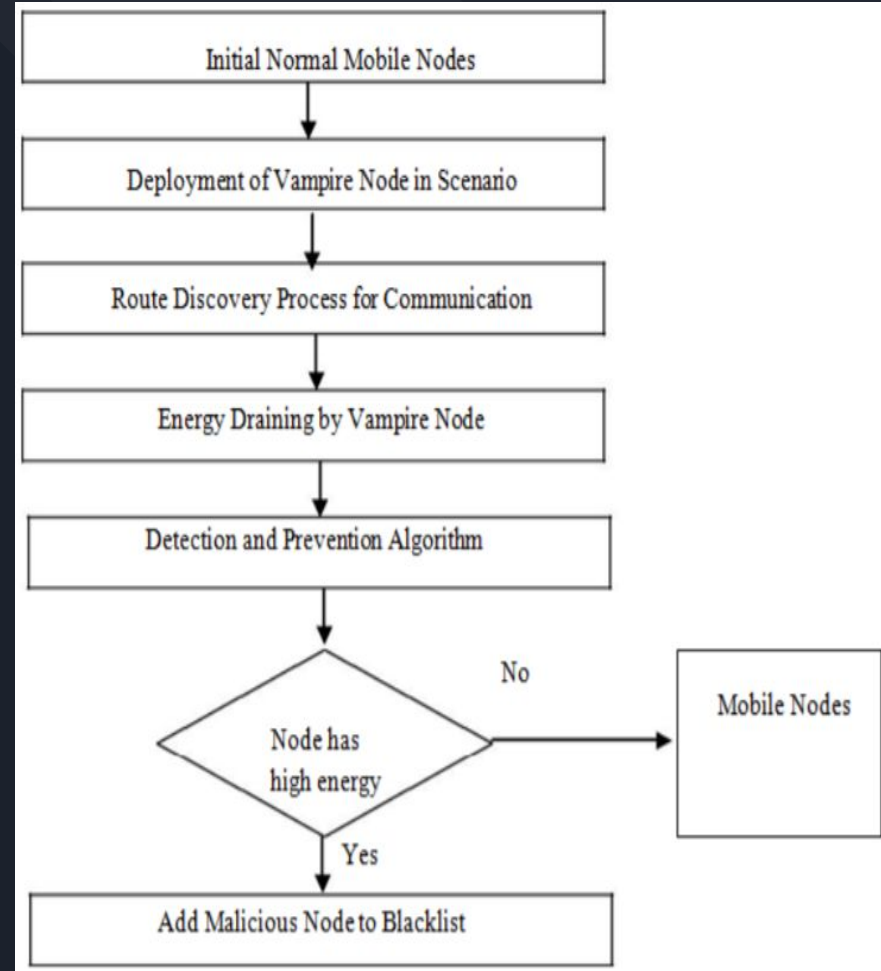
Network simulator - Used to understand the system behavior having complexity in traditional analytical methods. In the simulator, the network built with devices, links, applications, agent, etc. The simulation and data analysis observed using network animator and xgraph software.


NAM - Network animator is program simulation and data analysis observed using network animator and xgraph software.

- 
- ★ INTRUSION DETECTION SYSTEM TO IDENTIFY MALICIOUS NODE(S) INTO AD-HOC NETWORKS
 - ★ PROTECTION FROM VAMPIRE ATTACK ON ROUTING PROTOCOL

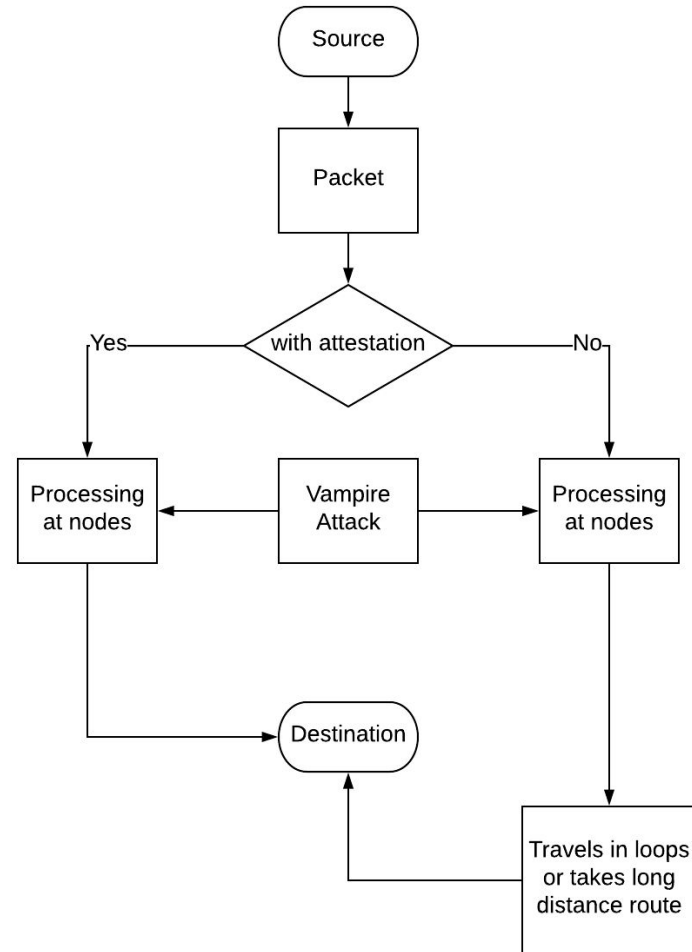
To be done...

★ INTRUSION DETECTION SYSTEM
TO IDENTIFY MALICIOUS
NODE(S) INTO AD-HOC
NETWORKS



- 
- ★ A NS2 .35 simulator should be used to develop and observe the performance of proposed sensor network scenario and prevention technique.
 - ★ "Generic" Energy model is to be configured to specify energy consumption at transmission, receiving, idle and sleeping stage.
 - ★ Keep track on battery consumption, introduce overload during attack and calculate natural and intentional power consumption.

★ PROTECTION FROM VAMPIRE ATTACK ON ROUTING PROTOCOL





What is already there?

PLGP

- Developed By Parno, Luk, Gaustad and Perrig (**PLGP**).
- Vulnerable to vampire attacks but can be modified to resist vampire attacks.



PLGP in presence of vampires:

- ★ Forwarding nodes don't know the path of a packet and allowing adversaries to divert packet to any part of the network.
- ★ Honest node may be farther away from the destination than malicious nodes.
- ★ But honest node knows only its address and destination address.
- ★ Vampire moves packet away from the destination.
- ★ Worse if packet returns to vampire as it can reroute.



What can be done?

No-backtracking implies Vampire resistance.

PLGP does not satisfy No-backtracking property.

No-backtracking property:

No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network.

Case 1: Honest node Honest node $\rightarrow \dots(\text{hops})\dots \rightarrow \text{Destination}$

Case 2: Malicious node Malicious node $\rightarrow \dots(\text{hops})\dots \rightarrow \text{Destination}$


- ★ Same no of Hops
- ★ Same network wide energy utilization
- ★ is independent of the actions of malicious nodes



So...

Propose PLGP with attestations (PLGP_a):

- ★ Add a verifiable path history to every PLGP packet
- ★ Every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node.
- ★ Every forwarding node verifies the attestation chain to ensure that the packet has never traveled away from its destination in the logical address space.



Simulation Parameters

Channel	Channel/WirelessChannel
Propagation	Propagation/TwoRayGround
Network Interface	Phy/WirelessPhy
Platform	Ubuntu 18.04
NS Version	Ns-allinone-2.35
MAC	Mac/802_11
Interface Queue	Queue/ DropTail / PriQueue
Link Layer	LL
Antenna	Antenna/OmniAntenna
Interface Queue Length	50 packets
No. of Nodes	10, 30, 50, 100, 150
Max Speed of Nodes	5 m/s
Simulation area size	500*500
Traffic Pattern	CBR Sessions
Packet Rate	60 pps
CBR Packet Size	64 bytes
Simulation Duration	20.0 seconds

Performance Evaluation Metrics

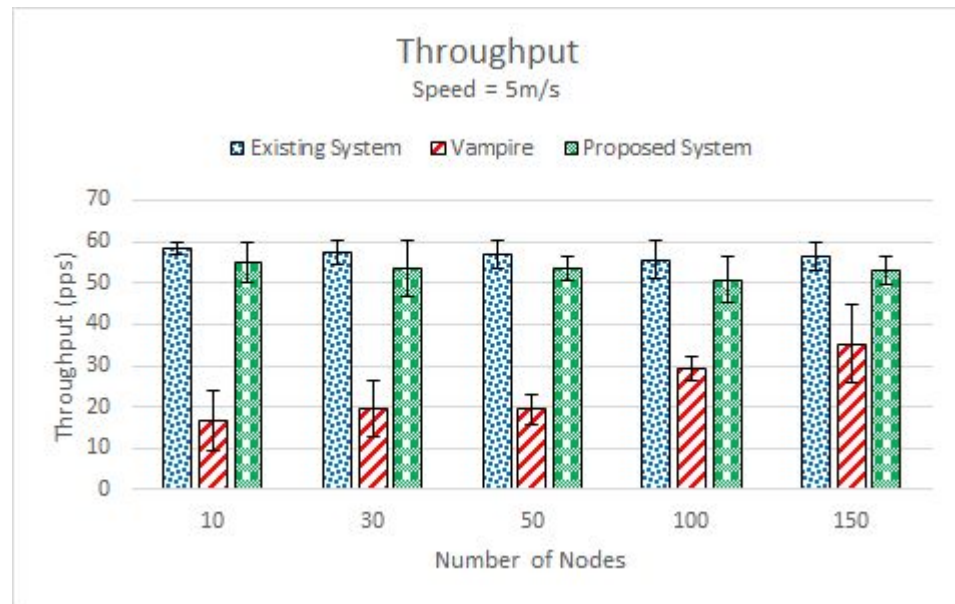
❑ Throughput:

Throughput is the number packets that have been received by the destination successfully in a given time period.

$$\text{Throughput [pps]} = \frac{\text{Number of received packets}}{\text{Data transmission period}}$$

Cont..

No. of Nodes	Existing System	Vampire	Proposed System
10	58.228857	16.515584	54.907701
30	57.45692	19.67692	53.601836
50	57.00404	19.527437	53.54307
100	55.6434747	29.361238	50.706913
150	56.558577	35.22077	53.06718





Performance Evaluation Metrics

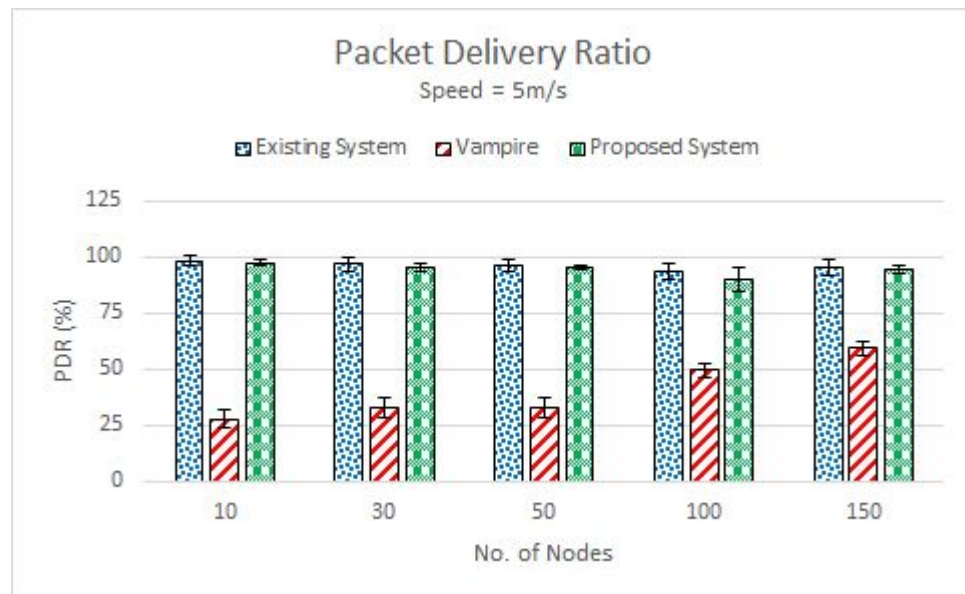
❑ Packet Delivery Ratio:

Packet Delivery Ratio indicates the ratio of number of packets which make to destination safely to the number of packets produced at the source.

$$\text{PDR} = \frac{\text{Sum of number of packets received}}{\text{Sum of number of packets sent}} * 100$$

Cont..

No. of Nodes	Existing System	Vampire	Proposed System
10	98.24573215	27.868215	97.527
30	96.9521758	33.202619	95.207525
50	96.1879895	32.9503817	95.1031412
100	93.8921864	49.5438296	90.06564895
150	95.4363195	59.431138	94.2578695





Performance Evaluation Metrics

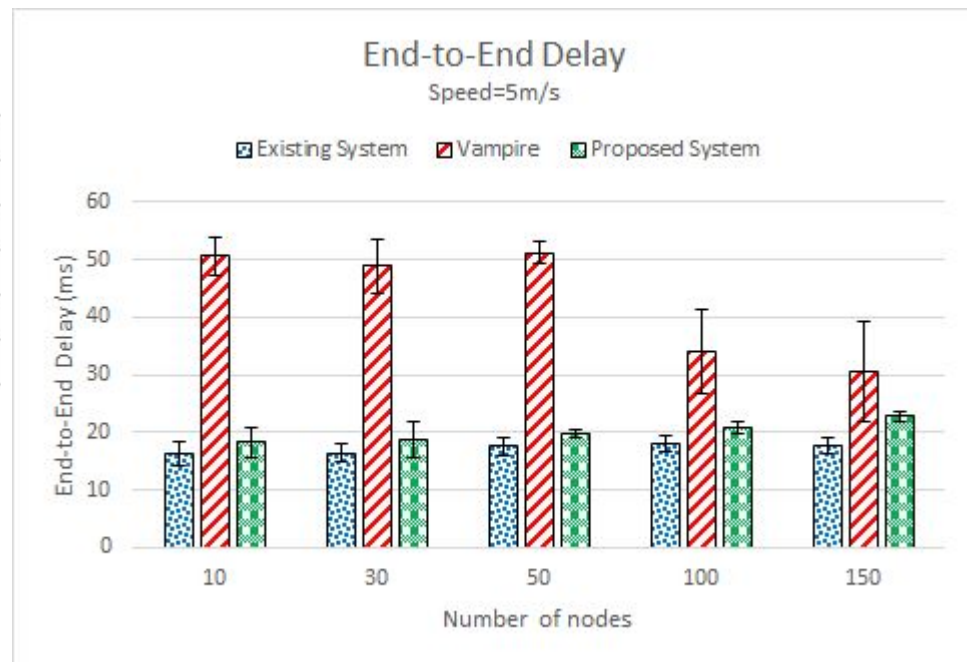
❑ End-to-end Delay:

End-to-end delay is defined as the average time consumed by a packet to travel from the packet creator to the packet destructor. It is calculated from when the packet arrives in queue. So, even the waiting period at queue is also included. It even considers the time taken for the route discovery process.

$$\text{End-to-End Delay [ms]} = \frac{\text{Data Transmission Period}}{\text{Number of received packets}} * 1000$$

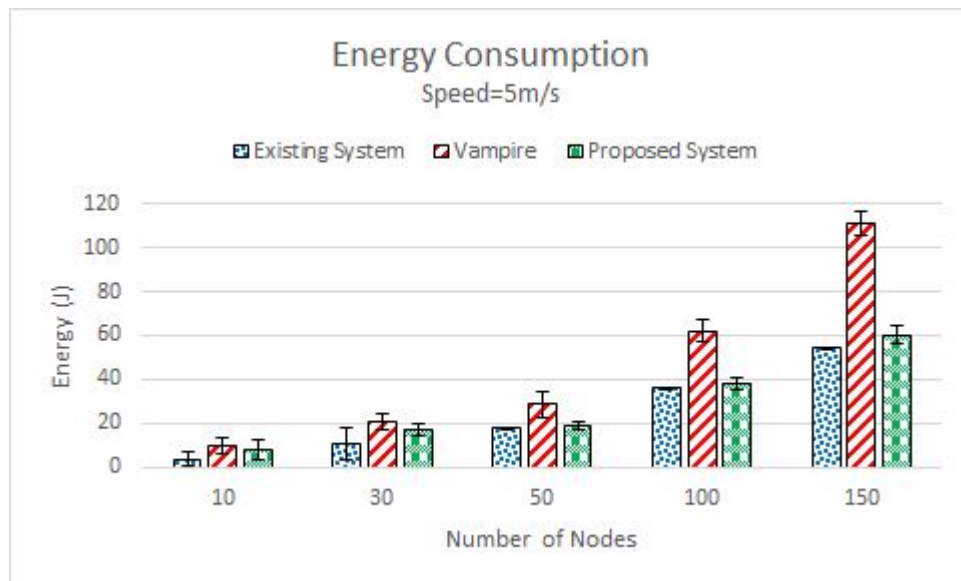
Cont..


Number of Nodes	Existing System	Vampire	Proposed System
10	16.17518869	50.54887217	18.21238154
30	16.40434367	48.82096047	18.65607718
50	17.54261625	51.2099982	19.67655381
100	17.97155921	34.05850943	20.72117686
150	17.68078438	30.3923385	22.8440386



Energy Consumption

No. of Nodes	Existing System	Vampire	Proposed System
10	3.767402	10.114437	7.888791
30	10.800211	20.532364	16.877696
50	18.1953719	28.578204	19.0348955
100	36.0648893	62.1851633	38.126623
150	54.4324595	110.7976	60.0554678



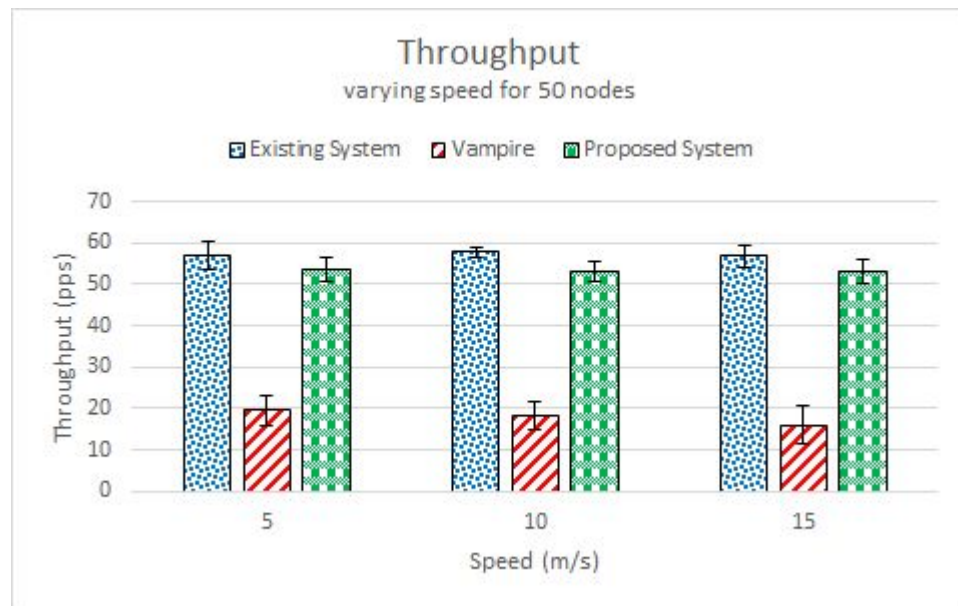


Simulation Parameters (for varying speed)

Channel	Channel/WirelessChannel
Propagation	Propagation/TwoRayGround
Network Interface	Phy/WirelessPhy
Platform	Ubuntu 18.04
NS Version	Ns-allinone-2.35
MAC	Mac/802_11
Interface Queue	Queue/ DropTail / PriQueue
Link Layer	LL
Antenna	Antenna/OmniAntenna
Interface Queue Length	50 packets
No. of Nodes	50
Max Speed of Nodes	5, 10, 15 m/s
Simulation area size	500*500
Traffic Pattern	CBR Sessions
Packet Rate	60 pps
CBR Packet Size	64 bytes
Simulation Duration	20.0 seconds

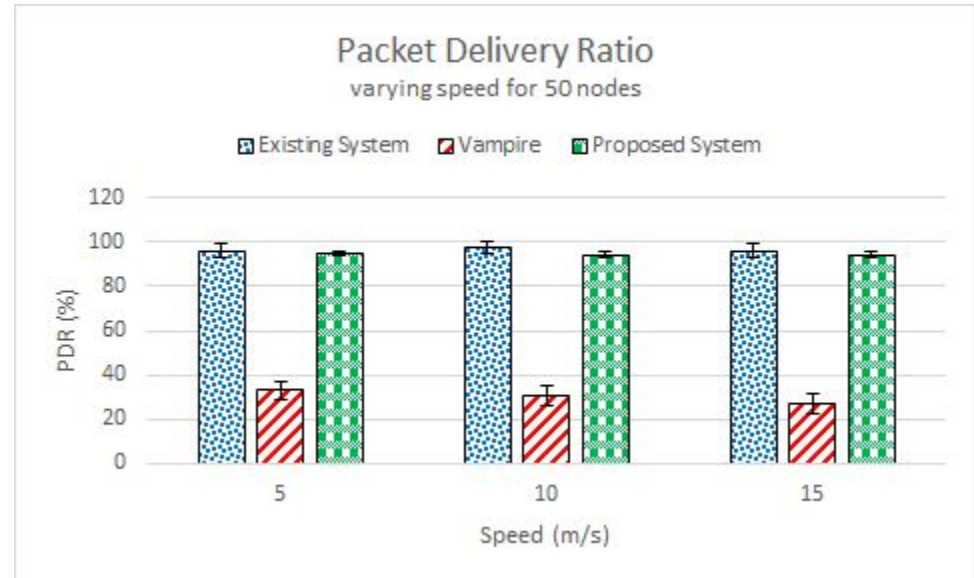
Throughput

Speed	Existing System	Vampire	Proposed System
5	57.0040401	19.527437	53.543069
10	57.801047	18.190832	53.133485
15	56.8185111	16.041174	53.105009



Packet Delivery Ratio

Speed	Existing System	Vampire	Proposed System
5	96.1879895	32.9503817	95.1031412
10	97.53285	30.69501	94.37564
15	95.87493	27.0677	94.32506





Conclusion

- Vampire attack is a Resource Depletion attack.
- Vampire attack is not protocol specific. Vampire attacks can be distinguished as: Carousel and Stretch Attack.
- Discovery of malicious nodes, is based upon energy drain in the network.
- To prevent the vampire attack, all the packets are attached with an attestation in the header, where the packet gets signatures from each and every node that it passes through which prevents the packet from reaching the same nodes again and again.
- The system performance has been evaluated using parameters such as throughput, packet delivery ratio and end-to-end delay for mobile nodes.



References


- [1] The network simulator — ns-2. <http://www.isi.edu/nsnam/ns/>.
- [2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.
- [3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure ondemand 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.



THANK
YOU



BACKUP SLIDES



PLGP does not satisfy No-backtracking property:

In PLGP packets are forwarded along the shortest route through the tree that is allowed by the physical topology.

Since the tree implicitly mirrors the topology and since every node holds an identical copy of the address tree, every node can verify the optimal next logical hop.

However, this is not sufficient for no-backtracking to hold, since nodes cannot be certain of the path previously traversed by a packet.

Adversaries can always lie about their local metric cost

PLGP is still vulnerable

Clean Slate Sensor Network Routing

Two phases:

- Topology Discovery Phase
 - Packet Forwarding phase
-
- ★ Discovery organizes nodes to trees
 - ★ Initially : each node knows only itself At end of discovery each node should compute the same address tree as other nodes.
 - ★ All leaf nodes are physical nodes in network and virtual addresses corresponds to their position in the network.

Topology Discovery Phase:

- ★ Every node broadcast certificate of identity including public key.
- ★ Each node starts as its own group size one ,with virtual address zero.
- ★ Groups merge with smallest neighbouring group
- ★ Each group chooses 0 or 1 when merge with another group.
- ★ Each member prepends group address to their own address
- ★ Gateway nodes
- ★ By end each node knows every nodes virtual address ,public key and certificate.
- ★ Network converges to a single group

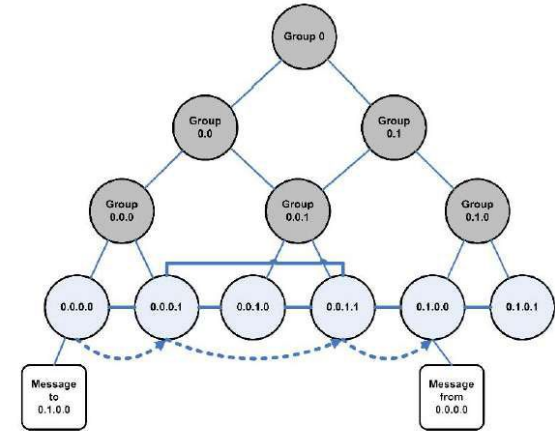


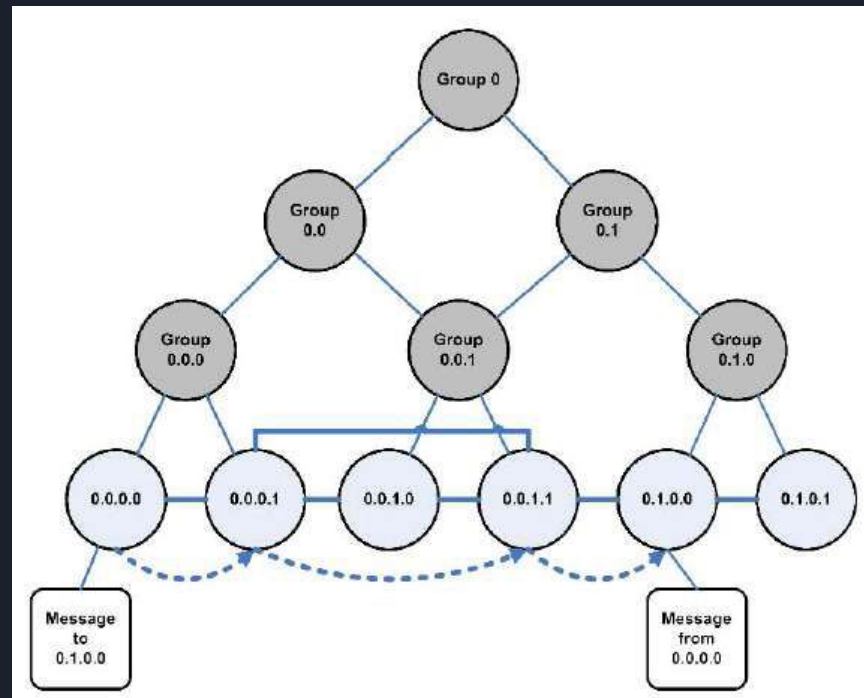
Fig. 6. The final address tree for a fully converged six-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that nonleaf nodes *are not physical nodes* but rather logical group identifiers.


Packet forwarding phase:

All decisions are made independently by each node

A node when receives a packet determines next hop by finding the most significant bit of its address that differs from the message originators address.

Every forwarding event shortens the logical distance to destination





Step 1: Broadcast the message RREQ Packet end to all the nodes and check which have the shortest path for the communication. RREQ message is broadcasted in the network.

Step 2: Receive Reply message. Destination sends the RREP message to the source. RREP message is unicast to source.

Step 3: Compare energy level of each node. All the nodes will have the same energy level rather to the vampire node. Vampire node will have the highest energy level in compare to the other nodes energy level.

Step 4: If node has highest energy level

4.1 Detection

Get the particular node id from the routing table which have the highest energy level.

4.2 Prevention

Add node as a Vampire Node and find another route to send message.

Step 5: Else, Accept Node as legitimate node. If all nodes have the same energy level means all the nodes are legitimate nodes.

Step 6: Stop



Research Timeline

Activities	January, 2018	February, 2018	March, 2018	April, 2018
Introduction				
Literature Review				
Methodology				
Proposal				
Modification of Algorithm				
Experimental Results				
Research Submission				