In MANET, A Trust-Based Mechanism Using The AODV Protocol Is Used To Prevent Black-Hole Attacks.

Paras Nath Mishra, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- dr. paras.m@arkajainuniversity.ac.in

ABSTRACT: A mobile ad-hoc network is a collection of mobile nodes that may connect without the need of fixed infrastructure; because of this, it is vulnerable to different assaults. The black hole attack is a dangerous security issue that increases network overhead and disrupts normal network operation; under such situations, the TAODV routing protocol is preferred. TAODV (Trust Based Ad-hoc Network) is utilized in this study to analyze various traffic patterns such as CBR, Exponential, and Pareto. Indoor shadowing is utilized as a propagation environment, and various Quality of Services are observed (QoS). A black hole is a region of space-time where gravity is so strong that nothing can escape it, including particles and electromagnetic radiation like light. A sufficiently compact mass can deform space-time to form a black hole, according to general relativity theory. The event horizon is the point at which there is no way out. Although it has a huge impact on the fate and circumstances of an object passing through it, it has no locally detectable features, according to general relativity. A black hole is similar to an ideal black body in that it does not reflect light. Furthermore, in curved space-time, quantum field theory predicts that event horizons emit Hawking radiation, which has the same spectrum as a black body with a temperature that is inversely proportional to its mass. For black holes of stellar mass, this temperature is on the order of billionths of a Kelvin, making direct observation nearly impossible. Objects with gravitational fields that are too strong for light to escape were first considered by John Michel and Pierre-Simon Laplace in the 18th century. Karl Schwarzschild discovered the first modern solution of general relativity that would characterize a black hole in 1916, and David Finkelstein published the first interpretation of it as a region of space from which nothing can escape in 1958. Black holes were once thought to be a mathematical curiosity; theoretical work in the 1960s revealed that they were a generic prediction of general relativity. Jocelyn Bell Brunel's discovery of neutron stars in 1967 piqued interest in gravitationally collapsed compact objects as a possible astrophysical reality. Cygnus X-1 was the first known black hole, discovered in 1971 by several researchers independently.

KEYWORDS: MANET, TAODV, Mobility Model, Shadowing and Gauss Markov Mobility.

1. INTRODUCTION:

MANETs (mobile ad-hoc networks) are wireless systems that are self-contained and dispersed. Laptops, mobile phones, personal digital assistants, and personal computers are examples of nodes. The nodes may serve as both a router and a host, or they can do both at the same time. They create inconsistent topologies with each other in the network depending on the connection. MANET is an autonomous network. It is a collection of numerous devices that are capable of wireless communication and networking. It establishes a temporary link for data transfer between the computer and the devices[1].

In a mobile ad-hoc network, transmission may take place directly between two nodes or through a multi-hop route. The most essential issue for the fundamental operation of a mobile ad-hoc network is security. Assuring that security problems have been addressed may result in the data being kept private and intact. MANETs are more susceptible to attacks because to intrinsic features such as open medium, cooperative algorithms, constantly changing topology, no defined defensive mechanism, and absence of central monitoring.

Their popularity is growing because to their dynamic nature, simplicity of deployment, and lack of infrastructural structure. It is based on the TCP/IP communication framework between communicating workstations. TCP/IP has been changed for MANET to make it more efficient. A new set of protocols has been developed to reduce end-to-end latency. For the researcher, a routing protocol in MANETs is an appealing and difficult study topic. MANET is divided into three types based on the routing protocols they use: hybrid protocol, reactive protocol, and proactive protocol.[2]

Management of Reputation

Modified AODV stands for trust-based ad-hoc on demand vector routing (TAODV), which is a secure routing system for mobile ad-hoc networks. As nodes execute trusted routing behaviors, TAODV has many characteristics, mostly based on the trust dependence among them. The whole network will identify and refute a node that engages in black hole activity.

Along with the trust function, the AODV routing protocol is implemented. The ability of nodes in a mobile ad-hoc network to communicate with one another is dependent on their neighbors' cooperation and confidence. An acceptable value of the node may be categorized as follows based on the security with a neighbor:

- Unreliable: The Unreliable is a node that is not trusted. Unreliable node is a node with a low degree of trust. When a node enters a network and its trust connections with its neighbors are poor, that node is first labeled as unreliable.
- Reliable: These are nodes with a trust rating in the range of Most Reliable to Unreliable. Only if it has received some packets from its adjacent node is a node deemed Reliable.
- Most Reliable: The most trustworthy nodes have the greatest degree of trust. 978-1-5090-0669-4/16/$31.00 2016 Symposium on Colossal Data Analysis and Networking (CDAN) IEEE

A higher trust level indicates that numerous packets were successfully received or sent by neighbors via this node. The trust value for all of anynode's neighbors is computed during the route discovery phase of the Ad hoc On Demand Distance Vector Routing protocol[3].

TAODV [1] is a new secure routing protocol designed by Xiaoqi Li. TAODV (Trusted AODV) is an extension of the AODV routing protocol that uses the concept of a trust model to safeguard routing behavior at the MANET network layer. Finally, they concluded that the trusted AODV routing protocol offers a lighter-weight but more versatile security solution than existing encryption and authentication schemes.

Arindrajit Pal investigates the behavior of mobile nodes at various speeds for various traffic patterns, including CBR, Exponential, and Pareto [2]. They found that AODV routing outperforms DSR routing, with throughput decreasing as node speed rises in both AODV and DSR routing. AODV routing's PDR is consistent across all traffic patterns. Figure 1 discloses the Packet Delivery Ratio with Gauss Markov Mobility[4]

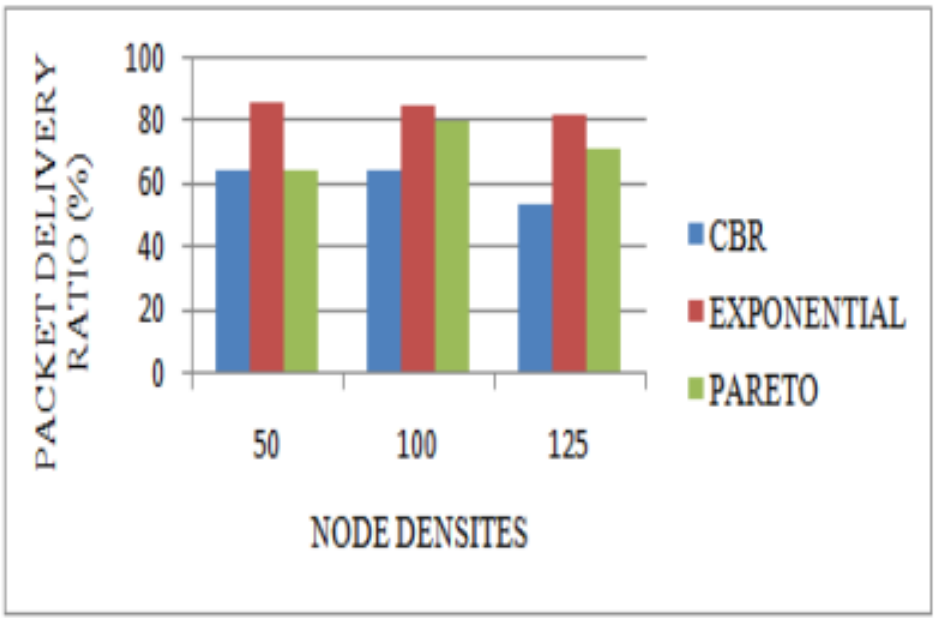

Table 1: Packet Delivery Ratio with Gauss Markov Mobility.

Table: Basis for deciding Trustworthiness of the Node

Most Reliable	Unreliable	Reliable	Action
		≥0.7	Request and check again
	<0.7		Disbelief the node
>0.7			Trusted node

2. DISCUSSION:

The TAODV algorithm is described in depth in the stages that follow.

Step 1: In a mobile ad-hoc network, nodes are linked to each other to relay messages. Every node starts with a Trust index of 0.7.

Step 2: The source node sends the route request packet to its neighbors so that messages may be relayed to the destination.

Step 3: If the route exists in the neighbor node's cache memory, it sends a route reply to the source node; if not; intermediate nodes transmit the identical route request to their neighbors and then to additional intermediate nodes until the destination is located.

Step 4: When the adjacent nodes send you a route reply message. The source node examines the sequence number and trust index of responding nodes before choosing the most reputable node to transmit messages to.

Step 5: The message is sent from the source node to the chosen neighbor nodes[5].

Step 6: When a message is delivered properly, the neighbor's trust value rises. The value of trust is reduced if it is not provided.

Step 7: Black hole nodes are defined as nodes with a trust index of less than 0.7, and these nodes are blacklisted.

Albert Einstein created his theory of general relativity in 1915, after previously demonstrating that gravity did affect light's velocity. Karl Schwarzschild solved the Einstein field equations, which describe the gravitational field of a point mass and a spherical mass, just a few months later. A few months later, Johannes Droste, a Hendrik Lorentz student, independently gave the identical solution for the point mass and wrote more extensively on its characteristics. This solution behaved strangely at what is now known as the Schwarzschild radius, when it became singular, implying that some of the Einstein equations' terms became infinite.

At the time, the nature of this surface was not fully understood. Arthur Eddington demonstrated in 1924 that the singularity vanished when the coordinates were changed, but it took Georges Lemaître until 1933 to understand that this indicated the singularity at the Schwarzschild radius was a non-physical coordinate singularity. In a 1926 book, Arthur Eddington did comment on the possibility of a star with mass compressed to the Schwarzschild radius, noting that Einstein's theory allows us to rule out excessively large densities for visible stars like Betelgeuse because the Schwarzschild radius is so small "A star with a radius of 250 million kilometers could not possibly have the same density as the Sun. For starters, the gravitational pull would be so strong that light would be impossible to escape, and rays would fall back to the star like a stone to the earth. Second, the spectral lines' red shift would be so significant that the spectrum would be rendered obsolete. Third, the mass would cause the space-time metric to curve so much that space would shut up around the star, leaving us outside .Subrahmanyan Chandrasekhar estimated in 1931 that a non-rotating body of electron-degenerate matter over a specific limiting mass (today known as the Chandrasekhar limit at 1.4 M) had no stable solutions using special relativity[6].

Many of his contemporaries, such as Eddington and Lev Landau, disagreed with him, arguing that the collapse will be stopped by some undiscovered cause. They were partially correct: a white dwarf with a mass slightly more than the Chandrasekhar limit would collapse into a neutron star, which is stable in and of it. However, in 1939, Robert Oppenheimer and others predicted that neutron stars above a certain limit would collapse even more, based on Chandrasekhar's arguments, and concluded that no physical law would intervene to prevent at least some stars from collapsing into black holes. Their first estimates, based on the Pauli exclusion principle, put it at 0.7 M; however, after taking into account strong force-mediated neutron-neutron repulsion, the estimate was increased to 1.5 M to 3.0 M.The TOV limit estimate has been revised to 2.17 M based on observations of the neutron star merger GW170817, which is believed to have produced a black hole soon thereafter[7]

The singularity at the Schwarzschild radius's border was interpreted by Oppenheimer and his co-authors as suggesting that this was the boundary of a time-stopping bubble. For external viewers, this is a legitimate point of view, but not for infilling observers.[8] Since of this characteristic, collapsed stars were dubbed "frozen stars," because an observer from the outside would perceive the star's surface frozen in time at the moment of its collapse to the Schwarzschild radius[3].

Golden epoch this part concentrates on the simulation findings and their interpretation, which were obtained using Network Simulator 2. Performance indicators such as packet delivery ratio and throughput may be used to assess the behavior of a simulated intrusion-based black hole attack. In this part, we will look at an indoor obstructed shadowing model and construct trust-based AODV under various traffic conditions such as CBR, Exponential, and Pareto. The following are the results of the Trust Based AODV routing protocol for various traffic circumstances and mobility models such as Gauss Markov Mobility and Random Walk Mobility: It's the proportion of delivered packets to total packets sentries Scenario 802.11 Propagation Shadowing Model Simulation Tool NS-2.35There are 50 nodes, 100 nodes, and 150 nodes in the network.CBR, Exponential, and Antenna Omni directional Traffic Type IEEE 802.11 Routing Protocol TAODV Queue Limit 50 Packets MAC Type2000*2000 simulation area (in meters)Drop tail Channel Wireless Channel Queue type2016 Symposium on Colossal Data Analysis and Networking simulation time: 900 seconds (CDAN)The pace at which a successful message is delivered across a communication link is known as throughput. It's typically expressed in kilobits per second (kbps). Figure 2 discloses the Packet Delivery Ratios with Random Walk Mobility[9].

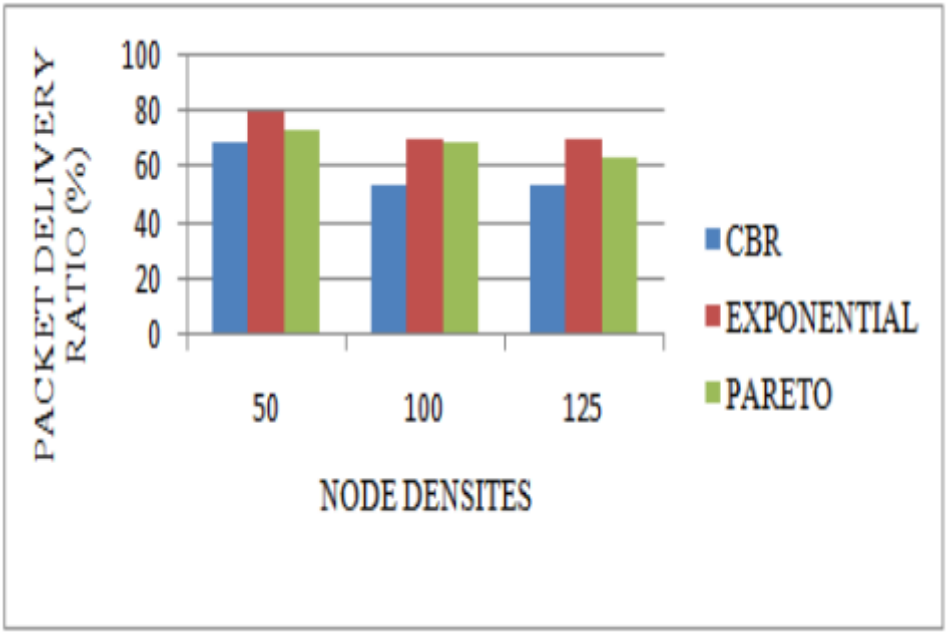

Figure 2: Packet Delivery Ratios with Random Walk Mobility[10]

Simulation Tool	NS-2.35
IEEE Scenario	802.11
Propagation	Shadowing Model
Network area	50 nodes, 100nodes and 150 nodes
Traffic Type	CBR, Exponential and
Antenna	Omni directional
MAC Type	IEEE 802.11
Routing Protocol	TAODV
Queue limit	50 Packets
Simulation area (in meter)	2000*2000
Queue type	Drop tail
Channel	Wireless Channel
Simulation time	900 Sec

3. CONCLUSION:

The trust-based AODV (TAODV) routing protocol is used to mitigate the effects of a Black Hole attack in this study. If the behavior of nodes is based on the Gauss markov mobility model, exponential traffic conditions are preferred to achieve the best result in terms of packet delivery ratio and throughput in an indoor environment. If the behavior of nodes is based on the Random walk mobility model, exponential traffic conditions are preferred to achieve the best result in terms of packet delivery ratio and throughput in an indoor environment. The no-hair theorem states that once a black hole has reached a stable state after creation, it has just three independent physical properties: mass, electric charge, and angular momentum; otherwise, the black hole is featureless. If the hypothesis is correct, any two black holes with the identical values for these characteristics, or parameters, are indistinguishable. The degree to which the hypothesis holds true for actual black holes under contemporary physics rules is still an open question.

REFERENCES:

[1] X. Calmet and R. Casadio, "What is the final state of a black hole merger?," *Mod. Phys. Lett. A*, 2018.

[2] Y. F. Yuan, "Black hole binaries in the universe," *Scientia Sinica: Physica, Mechanica et Astronomica*. 2017.

[3] J. van Dongen and S. de Haro, "On black hole complementarity," *Stud. Hist. Philos. Sci. Part B - Stud. Hist. Philos. Mod. Phys.*, 2004.

[4] P. Bueno and P. A. Cano, "Universally stable black holes," *Int. J. Mod. Phys. D*, 2017.

[5] A. B. Nielsen, "Black holes and black hole thermodynamics without event horizons," *Gen. Relativ. Gravit.*, 2009.

[6] J. L. Bernal, A. Raccanelli, L. Verde, and J. Silk, "Signatures of primordial black holes as seeds of supermassive black holes," *J. Cosmol. Astropart. Phys.*, 2018.

[7] D. Gaiotto, A. Strominger, and X. Yin, "5D black rings and 4D black holes," *J. High Energy Phys.*, 2006.

[8] Z. Xu, X. Hou, and J. Wang, "Possibility of identifying matter around rotating black hole with black hole shadow," *J. Cosmol. Astropart. Phys.*, 2018.

[9] W. Z. Chao, "Quantum black hole," *Gen. Relativ. Gravit.*, 1998.

[10] D. Bak, M. Gutperle, and R. A. Janik, "Janus black holes," *J. High Energy Phys.*, 2011.