A STRONG SECURITY STRATEGY FOR WIRELESS AD HOC NETWORKS AGAINST A SELECTIVE DROP ATTACK

[1] SUTHRAME SOUMYA, [2]DR.V.BAPUJI

[12]vaageswari College Of Engineering, Telangana, India

[1]soumyasuthrame22@gmail.com [2]bapuji.Vala@gmail.com

ABSTRACT

A network that doesn't rely on current infrastructure is known as a mobile ad hoc network; the name is relatively new for an old technology. The origins of this technology can be found in the early 1970s DARPA PR Net and SURAN projects. The use of this technology in non-military communication contexts is the most recent development. Some of the other aspects of the technology, like as multicasting and security, have also been the subject of recent research. The "conventional" issues of routing and medium access control have also received a lot of creative solutions. In this paper, we intend to summarise the most recent developments in four areas of ad hoc networking technology: routing, medium access control, multicasting, and security. Discussion is also offered when contrasting the suggested protocols.

INDEX TERMS: Wireless ad-hoc network, resistive to selective drop attack, network security, elliptic curve digital signature algorithm

I. INTRODUCTION

Wireless ad hoc networks, or WANETs. Although the overall scale of such networks is theoretically and practically constrained, their decentralised nature makes them ideal for a number of applications where central nodes cannot be relied upon. They might also make networks connected to wireless networks more scalable.

Ad hoc networks can be quickly set up and require less configuration, making them helpful in emergencies like natural catastrophes or armed conflicts. Because there are adaptive and dynamic routing technologies, ad hoc networks can form quickly. By their purposes, wireless ad hoc networks can be further divided. Wireless ad hoc networks, or WANETs.

Although the overall scale of such networks is theoretically and practically constrained, their decentralised nature makes them ideal for a number of applications where central nodes cannot be relied upon. They might also make networks connected to wireless networks more scalable.

Ad hoc networks can be quickly set up and require less configuration, making them helpful in emergencies like natural catastrophes or armed conflicts. Because there are adaptive and dynamic routing technologies, ad hoc networks can form quickly. By their purposes, wireless ad hoc networks can be further divided. All communication will then be sent to the infected host, enabling it to discard packets at will [6]. Across a mobile ad-hoc network as well, hosts are particularly vulnerable to collaborative assaults, in which several hosts are compromised and deceive the other hosts on the network [7]. Selective drop attacks can be thwarted via the RSDA protocol by preventing nodes from getting overwhelmed. It accomplishes reliability in routing by either disabling the link as faulty or by locating a different, more efficient route to the target. To find a reliable factor to defend against the selective drop attack, the list of link weights is computed [5]. For instance, if a route's weight total is high, which indicates low reliability [8], the attacking node can be discovered. Each node records its own weight, and the sum is appended to the route request's payload. By calculating the reliability rate, malicious nodes can be separated from other regular nodes. Nodes can join and exit the network whenever they choose, regardless of place or time, and the infected node roams about a lot.

2) As a result, malicious behaviour is challenging to identify or monitor.

The investigation shows that node misbehaviour and grey hole attacks make node isolation a more difficult problem and may affect each node's connectivity.

II. RELATED WORKS

2.1.A cluster-based method for distributed job allocation based on consensus
AUTHORS: J. Wetherall and D. Smith

In this research, we discuss the Cluster-Formed Consensus-Based Bundle Algorithm (CFCBBA), a novel improvement to the Consensus-Based Bundle Algorithm (CBBA) (CFBBA). The goal of CF-CBBA is to reduce the amount of communication required to complete a distributed job allocation process by breaking the problem into smaller chunks and processing it in parallel clusters. It has been shown that while distributing employment, CF-CBBA requires less communication than baseline CBBA. It has been investigated how successfully a mission—a collection of tasks—is carried out by a group of robots. These three crucial task allocation factors have been looked at: The time needed to assign responsibilities; the quantity of communication necessary to meet

2.2. Design of the Aodv routing protocol implementation

AUTHORS:I.D.Chakeresand E.M.Belding-\sRoyer

Up until now, the majority of research on ad hoc routing protocols has only used simulation. One of the strongest justifications for employing simulation is the difficulty of creating genuine implementation. The code is contained in a single, easily accessible, and precisely specified logical component in a simulator. But creating an implementation requires the use of a complex system with various parts, many of which have little to no documentation. Along with understanding the routing protocol, the implementation developer must also be familiar with all of the system's parts and their complex relationships. Ad hoc routing approaches are extremely different from traditional routing protocols, hence a new set of characteristics must be developed to support the routing protocol. In this essay, we describe the.

III. DATASET DESCRIPTION

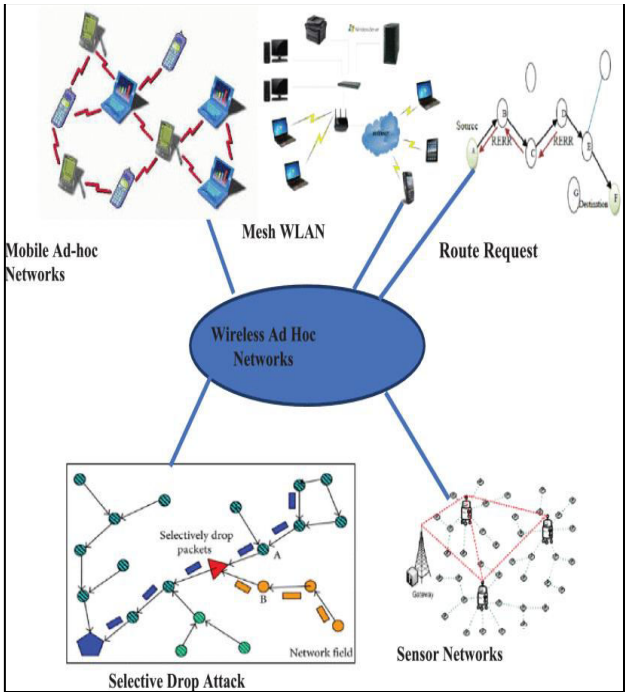


Fig 1:wireless AdHoc Networks

IV. METHODOLOGY

By deactivating the link with the largest weight and authenticating the nodes using the elliptic curve digital signature algorithm, it achieves reliability in routing. The packet drop rate, jitter, and routing overhead at a particular pause time are decreased to 9%, 0.11%, and 45%, respectively, using the suggested methods. In the RSDA system, the packet drop rates with one grey hole and two grey hole nodes are calculated to be 13% and 14%, respectively.

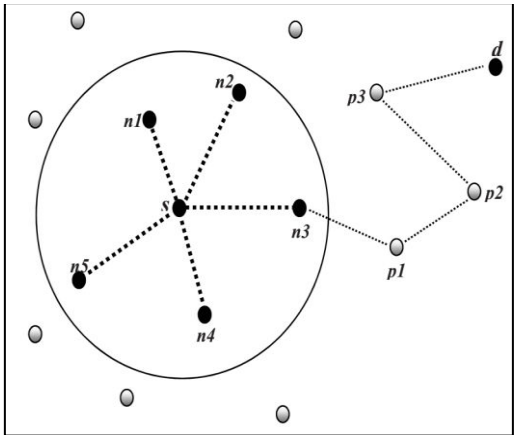


Fig 2:Failed or selfish node.

A.IMPLEMENTATION

The step of implementation is when the theoretical design is translated into a programmatically-based approach. The

application will be divided into a number of components at this point and then coded for deployment. Awt, Swings, and Socket programming are used in the application's front end, and My SQL was used as the back-end database. The following 5 modules make up the bulk of the application. They are listed below.

- **SOURCE MODULE**

The source node will attempt to browse the file in this module, choose the destination, and deliver the data to the router. Encrypt the file in Source while it is being uploaded, and then upload the file. All nodes' initialised file content will be available. Because text files can only be translated into packets in this situation, the source node selects the text file to transport to the destination.

- **ROUTER MODULE**

The router in this module is made up of four Networks, each of which has certain nodes. When the source sends a file, it first travels to Network 1 and passes through Network 1 nodes. If Network 1 node congestion is discovered, the file immediately switches to another node and travels to Network 2, Network 3, and Network 4 before arriving at the destination. View the Network specifics for more information on changing the energy size. The routing path and time delay can be seen in the router.

- **ROUTER MANAGER MODULE**

By examining the energy details and identifying attackers, ROUTER MANAGER views the attacker details in this module. This is used to offer a backup route in case an attack is discovered during data transmission.

- **DESTINATION MODULE**

This module uses a router to receive data from the sender. The destination node has a buffer location that is located in that application folder where it can save the data it receives.

- **ATTACKER MODULE**

In this module, the attacker chooses the network and the node, obtains the node's initial energy size, then alters it.

B.COMPARISON TABLE

Symmetric Technique Key Length	Asymmetric Technique Key Length	Elliptic Curve Key Length
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

V. EXPERIMENT, RESULTS, AND ANALYSIS

Fig1:Source Page.

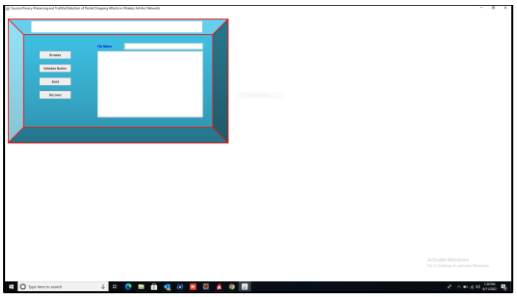


Fig2: Router :: Robust

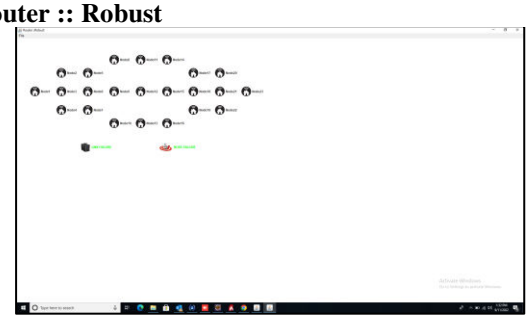


Fig3:Node A:: Robust

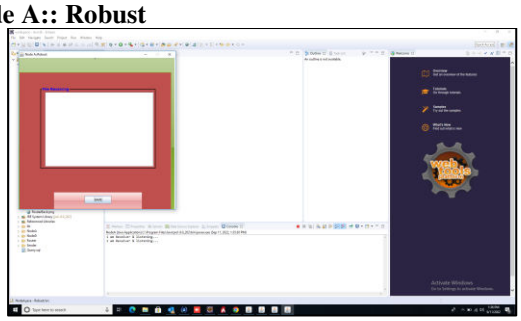


Fig3:Node B:: Robust

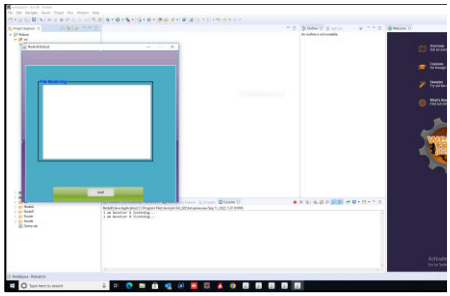


Fig3:Node C:: Robust

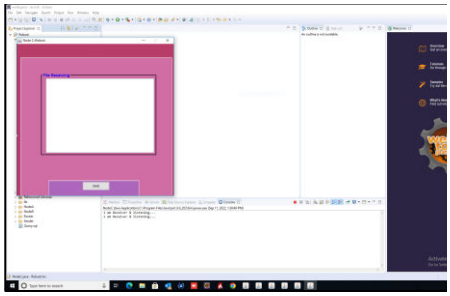


Fig3:Node D:: Robust

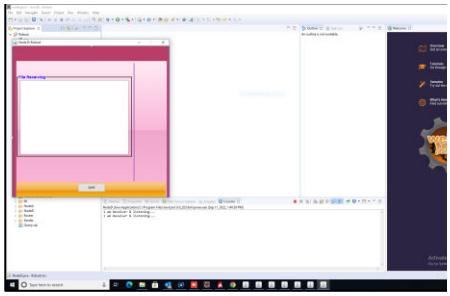


Fig3:Node E:: Robust

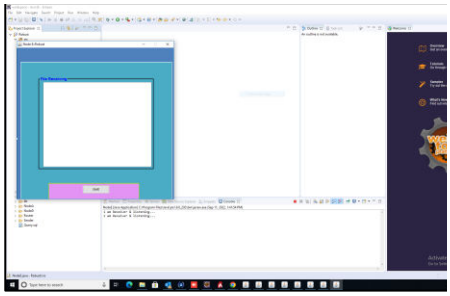


Fig3: Privacy-preserving and truthful detection of packet dropping attacks

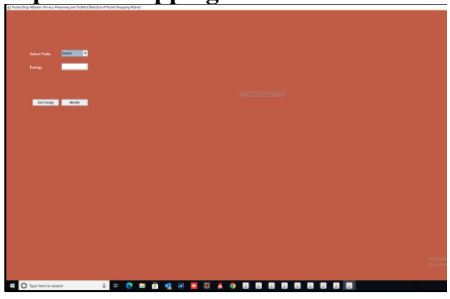


Fig4: AES.JAVA:: initialising nodes

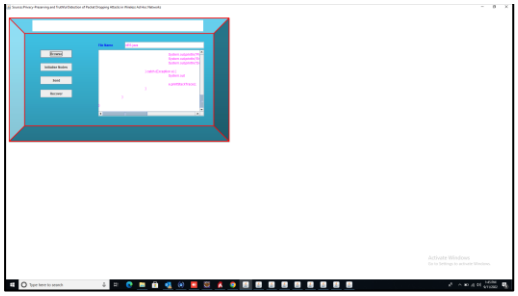


Fig5:Selecting Destination names

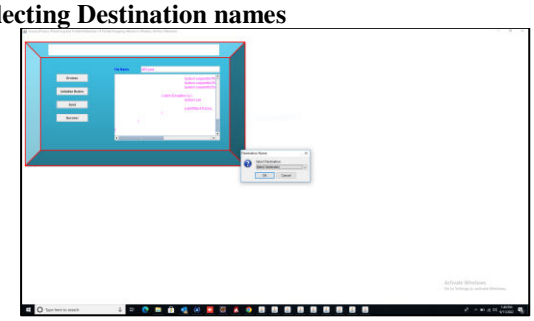
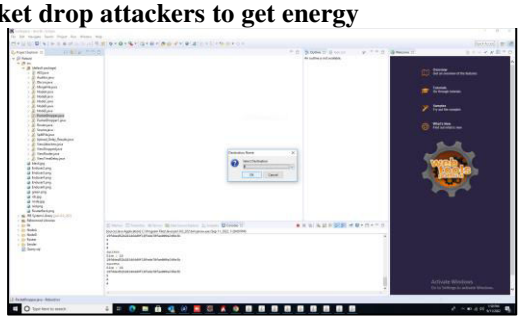


Fig6:Pocket drop attackers to get energy



VI. CONCLUSION AND FUTURE WORK

We ultimately came to the conclusion in this work that we suggested a resistant to selective drop attack (RSDA) strategy that can offer an efficient defence against selective drop attacks. Identification of the malicious nodes that overload a host and cut them off from the network by delaying its transmission process is crucial. Selective drop attacks may cause certain nodes to be unfaithful in their data transmission from source to destination nodes, and neighbouring nodes may not faithfully pass on their messages to the node after them. As a result, our suggested application may detect such malicious nodes right away and attempt to establish a different path away from the point of attack (POA) without interfering

with the original channel for sending the particular messages..

References:

[1]Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," Encycl. Telecommun., 2002.
[2] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in ITS Telecommunications Proceedings, 2006 6th International Conference on, 2006, pp. 761–766.
[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, 2002.
[4]I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Comput. networks, vol. 47, no. 4, pp. 445–487, 2005.
[5] V. Balakrishnan and V. Varadharajan, "Packet drop attack: A serious threat to operational mobile ad hoc networks," in Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, 2005, pp. 89–95.
[6] M. Peng, W. Shi, J.-P. Corriveau, R. Pazzi, and Y. Wang, "Black hole search in computer networks: State-of-the-art, challenges and future directions," J. Parallel Distrib. Comput., vol. 88, pp. 1–15, 2016.
[7]J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Syst. J., vol. 9, no. 1, pp. 65–75, 2015.
[8]A. Aijaz and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," IEEE Internet Things J., vol. 2, no. 2, pp. 103–112, 2015.
[9]P. Chen, S. Cheng, and K. Chen, "Information Fusion to Defend Intentional Attack in Internet of Things," IEEE Internet Things J., vol. 1, no. 4, pp. 337–348, 2014.
[10]X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," Am. Control Conf. (ACC), 2013, no. 1, pp. 3002–3007, 2013.