ISSN 2063-5346

A DISTRIBUTED NODE CLUSTERING COALITION GAME FOR MOBILE AD HOC NETWORKS

V.P.Kolanchinathan[1], T.R .Dinesh Kumar[2], Siva Saravana Babu S[3] , Abinaya.D[4],Divya sree.S[5],Vidhya.V[6]

Article History: Received: 01.02.2023 **Revised:** 07.03.2023 **Accepted:** 10.04.2023

Abstract

The two most well-known techniques for addressing the scalability issues in this research, which concentrate on unstructured networks, are Ad hoc wireless networks and clustering. This study investigates the clustering technique to manage enduring clusters for structured networks under size restrictions. We noticed that there was no formal basis for ad-hoc network clustering in the literature. Our research closes this gap by promoting the application of Cooperative game theory connecting players' clusters, and alliances to nodes. For this theoretical context, we can create a special clustering algorithm for scattered nodes in general. This algorithm, which has been shown is founded on the idea of switch operations, in which nodes decide whether or not to leave their coalition based on the effectiveness of the alliance. A transferable capability is present in the coalition-forming game, and these choices are made independently on each node. This general approach is therefore chosen for carefully defining their value functions and the heuristics used to choose the appropriate switch operations, both structured and unstructured networks can be efficiently used. according to these detailed Through simulations, we demonstrate which we suggested results work better than those currently in use, particularly the size and stability of the cluster.

vpkolanchinathan@velhightech.com[1], trdineshkumar@velhightech.com[2], sivasaravanababu@velhightech.com [3], anushree250401@gmail.com [4] , divyasmji@gmail.com[5], vidhya2066@gmail.com [6]

[1] [2] [3]Assistant Professor, Department of Electronics and Communication Engineering,

(Vel Tech High Tech Dr Ranagarajan Dr Sakunthala Engineering College, Chennai, India)

[4,5,6] UG Student, Department of Electronics and Communication Engineering,

(Vel Tech High Tech Dr Ranagarajan Dr Sakunthala Engineering College, Chennai, India)

DOI: 10.31838/ecb/2023.12.s1.167

I. INTRODUCTION

This study focuses on the mobile ad hoc network clustering issue.[1] Mobile adhoc networks rely on node mobility to create reliable, scalable and adaptable clusters which it is based on group mobility. Organizations that cluster messages are advised in order to lessen their message overflow in MANET [2].

Controlling overcrowding and making logy repairs quickly are two benefits of grouping MANET into MN s [3]. Cluster MN partitioning is a multi-objective optimization issue when the MANET size is large [4].

It is particularly appropriate for showing patterns of group mobility where behaviours like group division and merging are common among moving clusters [5].

We take into consideration two different Ad hoc networks that can be unstructured, where there is no particular network organisation and every node are equal, or structure, where there is a specific network organisation, where operational groups are present in which the components are such as squads or sections, and where there is an inherent hierarchical structure connected to their raison.

Military networks and PPDR are two examples of organized networks. In these networks, we presume that every component only participates in a single functional team. A group will be used to refer to a practical organisation for the sake of readability.

The presence of organizations highlights duo key distinctions from unstructured networks. First, traffic is primarily centred within groups.

The groupings within the network significantly impact how traffic is organized. Second, it is very probable that nodes from the same group will move in the same direction.

Making use of group knowledge when designing clustering solutions is advantageous for these two reasons, as it leads to more stable networks and superior service quality from start to finish (QoS)

Unstructured networks have been the subject of the majority of ad hoc network grouping studies to date. For instance, the cluster head node is the node in the surrounding region with the lowest identity and highest degree, according to the authors' suggested methods for the lowest identifier (LID) and highest degree clustering (HC).

2. EXISTNG SYSTEM:

Multi-hop wireless networks are ad hoc networks**.** without an infrastructure, every place point takes part as a result of sending and sharing information with other nodes. Self-organizing systems like those in military systems, vehicle networks, public protection and disaster relief (PPDR), and wireless sensor networks (WSN) are used when conventional infrastructure is unavailable or not appropriate. nodes forming clusters (also known as grouping) came first. suggested HF packet radio networks in the early 1980s and has since sparked a lot of research in the literature to create truly enormous ad hoc networks.

3. PROPOSED SYSTEM:

We have observed that there is no overarching theoretical paradigm for the study of ad hoc network clustering. In fact, the majority of the suggestions are protocol-focused and consider the CH poll. These depictions are so different from one another that it makes it challenging to analyze, compare, and extend them theoretically (for example, by studying their convergence). In this article, we suggest applying coalition game theory, which seems appropriate for such a framework, and generating our algorithms in accordance.

4. BLOCK DIAGRAM

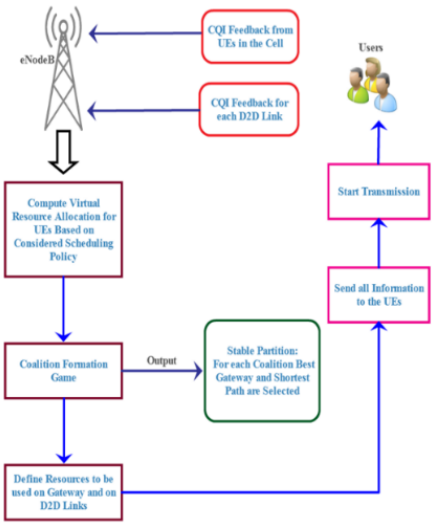


Fig 4.1 Block Diagram

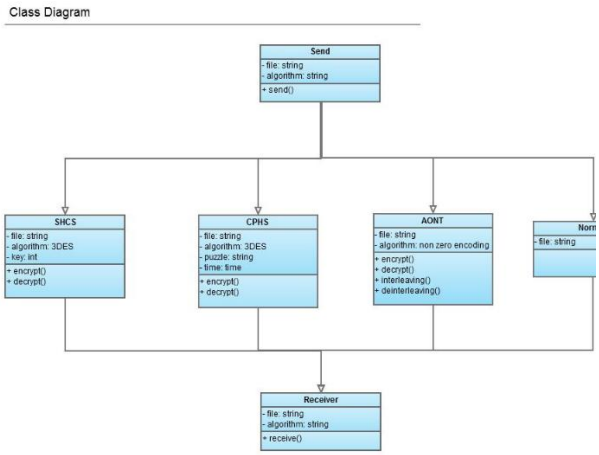


Fig 4.2 Class Diagram

A class diagram The UML utilizes a static structural diagram to depict the system's classes, attributes, and class interactions, providing an overview of the system's structure. Private visibility conceals information from external sources, while public visibility grants access to all the UML and utilizes a static structural diagram to depict the system's classes, attributes, and class interactions, providing an overview of the system's structure. Private visibility conceals information from external sources, while public visibility grants access to all. other classes to view the marked information A class diagram displays the interdependencies in the source code between classes (UML). A class diagram arranges the classes according to characteristics that are comparable.

5. METHODOLOGY

5.1 NETWORK MODULE: Network component we tackle the issue of limiting J's capacity to do selective jamming by prohibiting The node that jams the real-time classification of M.A. group of nodes is joined by wireless links to form the network. If nodes are within communication range of one another, they can communicate directly, or indirectly through a series of hops. Nodes can communicate in both broadcast and un-cast modes. There are two types of communication: encrypted and unencrypted. All intended receivers share symmetric keys for encrypted broadcast communications. The establishment of these keys can be achieved through either pre-shared pair-wise keys or asymmetric cryptography.

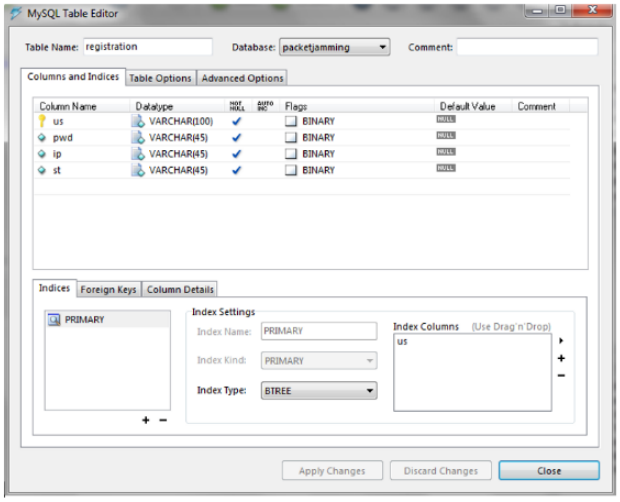


Fig 5.1 Network Module

5.2 REAL-TIME APPLICATION: Before being transmitted across the wireless channel, In the PHY layer, message M undergoes modulation, interleaving, and encryption. The receiver then performs signal demodulation, de-interleaving, and decoding to retrieve the original packet M. Therefore, even if a hiding scheme's

encryption key remained a secret, packet categorization may still be possible as a result of the static components of sent packets. This is because using the same key to encrypt a prefix plaintext produces a static cypher text prefix for encrypting data effectively computationally techniques like Block encoding. Therefore, an attacker who is familiar with below protocol specifications (the frame's construction) can classify the communications an email packet using the static cypher text sections of the packet. As soon as they receive the first block of encrypted text, Anyone with access to the decryption key can start the decryption process.

Fig 5.2 Login user

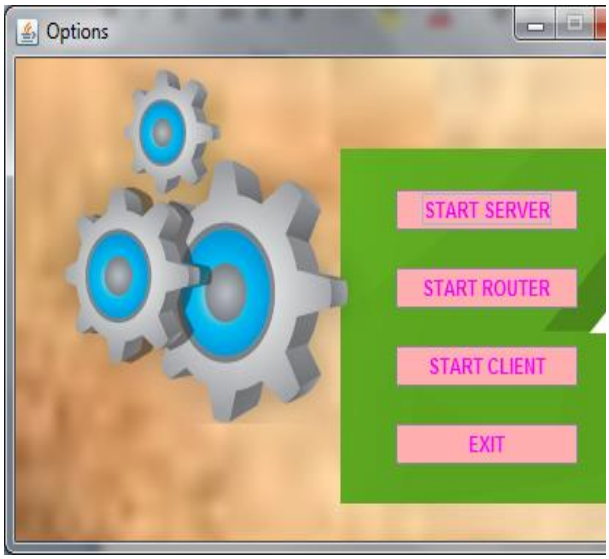


Fig 5.3 Server login

5.3 SELECTIVE JAMMING MODULE: We provide an example of how targeted jamming attacks affect the functionality of the network. Develop targeted jamming attacks for wireless networks with two hops. First, an attack was made on a TCP connection established across a multi-hop wireless network. Selective jamming in the second scenario would encrypt sent packets (including headers) using a static key and target network-layer control messages relayed during the route establishment process. This static decryption key, however, is vulnerable to compromise because it must be known by all intended recipients for broadcast communications. An opponent can begin decrypting as soon as they receive the first block of encrypted text if they have the decryption key. We provide an instance of how targeted jamming attacks affect the functionality of the network. Develop targeted jamming attacks for wireless networks with two hops This static decryption key, however, is vulnerable to compromise because it must be known by all intended recipients of the broadcast.

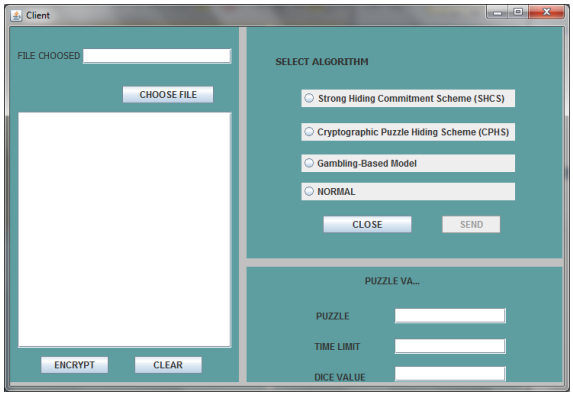


Fig 5.1 Selective Jamming

5.4 CRYPTOGRAPHIC PUZZLE HIDDING SCHEME: We offer a packet-concealing method built around cryptographic conundrums. Such puzzles' principal goal is to make the solver perform a predetermined sequence of calculations before he may discover an important secret. A puzzle's difficulty and the solver's computational skills determine how long it takes to find the solution. The puzzle-based approach has the benefit that its security is independent of the PHY layer parameters. It does, however, have a higher overhead for computation and communication. We see a

handful of puzzle schemes as the CPHS's cornerstone. We look at the implementation details for each plan that affect security and effectiveness. In order to create a secret over an unsecured channel, Merkle first suggested cryptographic puzzles.

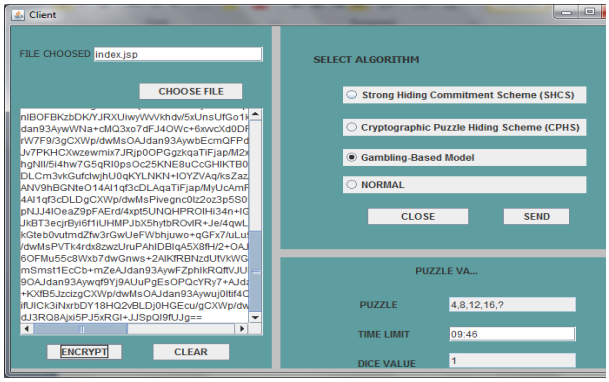


Fig 5.1 Cryptographic Puzzle

5.5 GAMBLING-BASED MODULE

To estimate this we develop a game-based approach to predict the time-critical application's message invalidation rate under jamming attacks. We can confirm our conclusions and look into the consequences of jamming attacks on an experimental power substation network by analysing a collection of use cases provided by the National Institute of Standards and Technology. (NIST). For the purpose of providing accurate theoretical and practical results, we develop the jamming attack detection based on estimation (JADE) system, which provides accurate and reliable jamming detection for the experimental substation network.

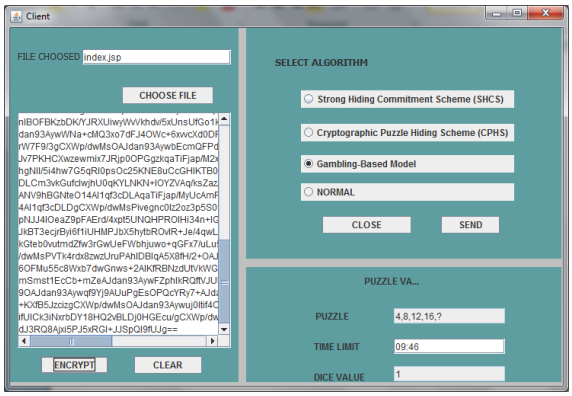


Fig 5.1 Gambling Module

6. RESULT

The optimal predictive model of crime is determined in the first step by using five classifier models. It is put into practice, and the outputs of every model of the ML algorithm comparisons are made. According to the results of the aforementioned studies, it was shown utilising the random forest algorithm when used in an ensemble manner, produces reliable prediction results on crime data. However, we propose a method for predicting crimes based on stacks (SBCPM) for the second stage after discovering the ensemble approach is less reliable while the stacking method is more.

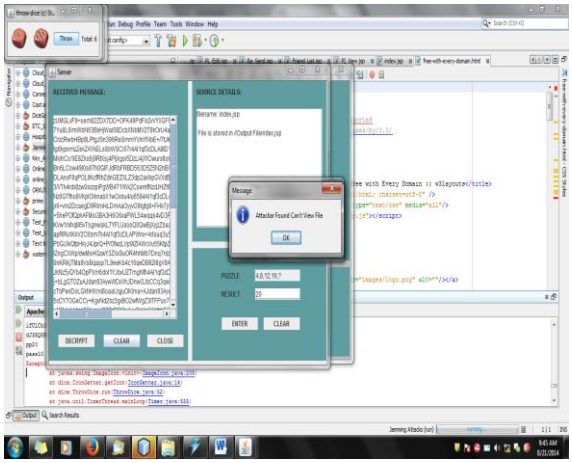
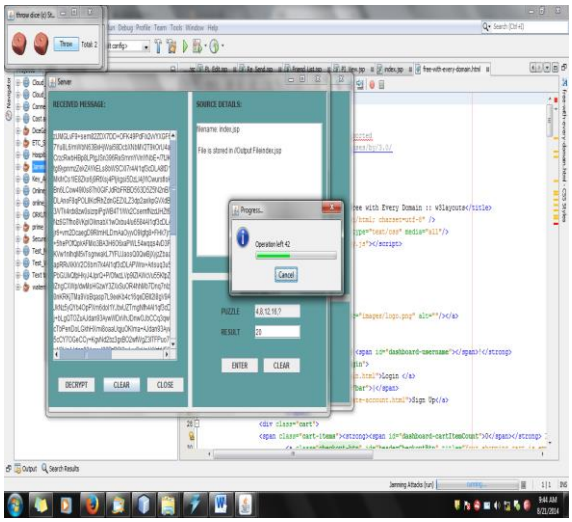


Fig 6.1 Final output



7. CONCLUSION

The rate of crime in our culture today is regularly rising day by day. Managing crime is a necessity because it is a natural aspect of human activity. It is improbable that human civilization would ever be completely free of criminals. This application is built to function effectively and successfully. It leads to rites and lucky actions against wrongdoing that are described. The data can supposedly be obtained quickly and accurately, as is common knowledge .Moreover, it ought to lay out better correspondence, reducing misbehaviour and making the entire process less tiresome. By using these programmes, people who are uneasy have the time to go to the police department's main office to complain about their own actual problems or any other concerns, where they can express their disagreements online

REFERENCES

[1] G. Noubir, R. Rajaramanand, B. Sheng, and B. Thapa, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming," Proc. ACM Conf. Wireless Network Security (WiSec); 2011.

[2] M. Palaniswami, P. Hartel, J. Doumen, L.V. Hoesel, Y.W. Law, P. Hartel, and P. Havinga, "Energy- Efficient Link-Layer Jamming Attacks against WSN MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009.

[3] S. Liu, M. Krunz, and L. Lazos, "Mitigating Control-Channel Jamming Attacks in Multi- Channel Ad Hoc Networks," Proc. Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.

[4] P. Ning, H. Dai, Y. Liu, and A. Liu, "Randomized Differential DSSS: Jamming- Resistant Wireless Broadcast Communication," Proc. IEEE INFOCOM, 2010.

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2007.

[6]. Dongmei Zhao, Zhangdui Zhong, Ni, and Minming. "MPBC: A mobility prediction-based clustering scheme for ad hoc networks." Vehicular Technology, IEEE Transactions on 60.9 (2011): 4549-4559.

[7]. Baker D. J., Wieselthier J. E., and Ephremides design concept for reliable mobile radio networks with frequency hopping signaling[J]. Proceedings of the IEEE, 1987, 75(1): 56-73.

[8]. Hussein A, Yousef S, Al-Khayatt S, et al. An efficient weighted distributed clustering algorithm for mobile ad hoc networks[C]//Computer Engineering and Systems (ICCES), 2010 International Conference on. IEEE, 2010: 221-228.

[9[R. Palit, P. Thulasiraman, E. Hossain Mobility-aware proactive low energyclustering in ad hoc mobile networks, in: Proc. of IEEEGlobalCommunicationsConferenc e 2004 (GlobeCom'04), vol. 6,Dallas, TX, USA, November–December2004, pp. 3426– 3430.

[10]. I. Stojmenovic, J.S. Gonzalez, G. Chen, F.G. Nocetti, Connectivity-based hopclustering in wireless networks, in: Proc. of the 35th Annual Hawaii International Conference on System Sciences, HICSS, Hawaii, 7–10 January 2002, pp. 188– 191.

[11]. Thomas, Naved Khan, Prithwish, Basu, and DC Little. "A mobility based metric for clustering in mobile ad hoc networks." Distributed computing systems workshop, 2001 international conference on, IEEE, 2001

[12]. Zhang Y, Ng J M, Low C P. A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks[J]. Computer Communications, 2009, 32(1): 189-202

[13]. Benmansour, Tariq, and Samira Moussaoui. "GMAC: Group mobility adaptive clustering scheme for Mobile Wireless Sensor Networks." Programming and Systems (ISPS), 2011 10th International Symposium on. IEEE, 2011.

[14]. Hong, SU Xiao-qiang NI. "Probability-based Mobility Model for Mobile Users." Microcomputer Information 6 (2011): 003.