JCST Journal of Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7728747

PERFORMANCE ENHANCEMENT FOR MOBILE AD HOC NETWORKS ROUTING WITH BAYESIAN INTERFACE

Atma Prakash Singh
Ph.D. Research Scholar, Maharishi University of Information Technology Lucknow

Dr. Santosh Kumar
Professor, Maharishi University of Information Technology Lucknow

Abstract : In this Paper, we use probability theory to analyse the challenge of trust management. In particular, Bayesian likelihood outperforms rule-based methods for describing confidence in sparse, self-organizing networks. In order to accurately estimate confidence among confused ideas, three methods are used. Bayesian inference, Bayes networks and the Dempster-Shafer model (DST). To begin, let's imagine a mobile dedicated network (MANET) in which previously established relationships between trusted insiders are used for network penetration purposes. To determine which nodes in a MANET can be trusted based on their historical behaviour, we use Bayesian inference. The reliability of each node is determined based on its next probability. Direct and indirect evidence forms the basis of DST confidence assessment. A trust management system eliminates the threat posed by low-trust malicious nodes. We demonstrate that the suggested schemes provide better dynamic dependability, throughput, end-to-end latency, etc. under unfavourable circumstances than the state-of-the-art systems. To implement Manet's trust management tactics, we resort to the Bayesian networks framework. Examining the level of certainty that can be assigned to each node in a Bayesian network is essential when trying to simulate one. As a result, the bad actors will be contained inside the trust management system. In an effort to make spectrum sensing and data transmission safer, we examine several methods of providing trust management in ad hoc networks with CR capabilities. Using a consensus-based weighted approach, we increase the trustworthiness of collaborative spectrum sensing. The dangers to network security from NFV are also covered.

Keyword: Cloud computing, MANET, NFV.

1. Introduction : Mobile Ad hoc Networks

Military applications were the first to use mobile ad hoc networks. An improved likelihood of troop survival was the initial motivation for the design, which set out to establish a military tactical network that would operate under the harsh circumstances of a combat [1]. The modern warfare constantly prioritizes destroying established means of communication. Because MANETs are temporary networks, they might allow military communications like orders to reach the front lines without being intercepted or destroyed[2]. The exceptional adaptability of

MANETs suggests potential applications outside the military. As the price of routers and switches continues to decline, more and more industries are finding usage for MANETs.Separate public and private economic spheres. Then, MANETs may be utilized to help get the word out and get everyone working together after a disaster, like an earthquake, by creating temporary communication networks. MANETs operate independently of a central server, unlike traditional networks. Due to the lack of a centralized infrastructure, the many nodes in the network must depend on one another to convey data. In MANETs, nodes must cooperate not just to generate and receive information of relevance to them, but also to plan the dissemination of that information to other nodes.As there is no stationary infrastructure, it is crucial that all mobile nodes be aware of one other's presence while in radio range. Radio nodes that are physically close to one other are considered to be one-hop neighbours. If the nodes are relatively near to one another, the wireless connection might work in both ways[3]. Messages may only be sent and received between nodes that are physically linked to one another, or that are connected to one another via other nodes. Due to the transient nature of the nodes, the self-organized network may take on a variety of configurations. Nodes in the data route other than the source and the destination always forward data packets from the source to the destination nodes[3].

Below, we highlight certain MANET characteristics. [4].

- The network's nodes function separately from one another. The ability to join or exit the network is not restricted to any one node. Because of this, the topology of the network is always evolving.
- • To allow nodes to talk to one another, all other nodes must be cooperative. Each node may only send and receive information with its immediate neighbours. Since a result, multi-hop routing is a crucial strategy for MANETs, as it may coordinate nodes in a decentralized fashion to send packets throughout the network. The success of MANETs relies on their ability to self-generate and collaborate with one another.
- Each node's self-organizing, resource-constrained nature makes energy consumption a major issue. The longevity of MANETs is therefore determined by energy efficiency methods.
- The network may be deployed quickly and at little cost. This is why MANETs have better scalability than regular networks. When taking readings, MANETs may be utilized regardless of scale. This paper reviews the recent progress made in studying routing in MANETs. Assorted routing methods for

Multiple MANET protocols such as OLSR (versions 1 and 2) [5,6], DSR and AODV have been recognized by IEEE. After a quick introduction in Chapter 3, this section provides an in-depth look at OLSRv2. OLSRv2 [7] is the latest update to the OLSR proactive routing protocol. Multipoint routing (MPR), customizable communication metrics, and more message formats are some of the new additions to the original core OLSR algorithms built by OLSRv2. There are three basic components of OLSRv2, namely local area detection, MPR selection, and topology generation[8]. It complements the HELLO message and the topology control message [9]. One of the methods that a node uses to identify its wireless neighbours is neighbour discovery [10]. During the neighbourhood discovery process, HELLO messages are transmitted and may contain information about the state of the connection (whether symmetric, asymmetric, or multipoint relay)[11]. A node can establish bidirectional symmetric links with its nearest neighbours by transmitting periodic HELLO signals. In OLSRv2, we make two different types of MPR selection: damping and routing. Although multipurpose relays (MPRs) are most often used to speed up communication during a flood attack, they also contribute significantly to redirecting network control traffic[12]. If a node's neighbour selects an MPR stream, that neighbour's message is transmitted only once. Applying this strategy, it is possible to reduce network transmission volumes. With OLSRv2, MPR selection for routing is different from flooding and vice versa[13]. The main role of routing MPRs is to distribute communication status information through TC messages. This method offers the potential benefit of reducing the amount of network topology data that must be transmitted. The topology of a network is determined by the extent to which data about the state of its links is widely shared[14].

2. Bayesian Networks

Here, we provide an overview of Bayesian networks and its core concepts and jargon in order to show how they might be used to control trust in MANETs. A sort of graphical model called a Bayesian network may be used to simply depict the joint probability distribution of a large number of variables that may be connected to one another [15]. Bayesian networks thus combine elements of inductive reasoning with those of graph theory [16]. We can use a Bayesian network to analyse and evaluate trust by following Conditional probability distributions are generated and computed after three phases [17]: identifying a collection of state variables and their domains; creating a directed acyclic graph to link these variables; and so on[18].The direct acyclic graph (DAG) of a Bayesian network represents the state variables that define a hypothesis at each node. Any state variable may have either a discrete or continuous domain[19]. All areas are presumed to be discrete. Every possible combination of states is represented by two enormous capital letters. Usually (but not always), a direct link between two nodes in a network is taken to indicate a causal relationship [20]. One node's child receives each outgoing connection. Each vertex is connected to a probability distribution that depends on some other variable (CPD). All vertices, including those without parents, have CPDs in the presence of any events[21]. A Bayesian network's combined The probability of each state variable is determined by utilizing the chain rule [22].parent(x) is the collection of nodes of which x is a child, and X is the set of states in the Bayesian network.The backbone of Bayesian networks are the linkages between nodes, which may be either sequential or divergent or convergent [23]. Two of the A's and one of the B's produce the C in Fig. 1. According to the definition of Bayesian Networks, the aforementioned A, B, and C structure is an example of a sequential connection[24]. Knowledge of B implies familiarity with A and C, even if you are unfamiliar with the latter. This characteristic of the sequential connection is owed to the nature of the two-way communication they provide. Mathematically,

$$P(A,C|B)= P(A|B)P(C|B). \quad (1)$$

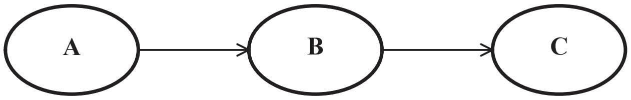

Figure 1: Sequential connection in a Bayesian network.

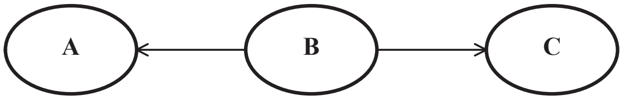

Figure.2: Diverging connection in a Bayesian network.

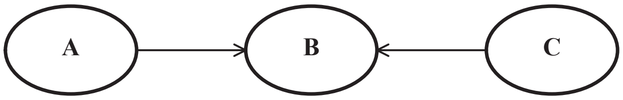

Figure 3: A Bayesian network with a converging link.

For each given hypothesis B, Bayesian networks use d-separation [25] to distinguish between hypotheses A and C. In the branching connection seen in Fig. 2, B is the parent of both A and C. With B present, A and C are able to undergo d-separation. Connecting route shown in Figure .3. B is the progeny of A and C in this definition. Converging links, one of the three kinds of linkages, are distinguished by several special characteristics. Only once B's identity as the child is confirmed can the dependency between A and C be established. A and C are d-connected with regard to B in a Bayesian network [25]. To describe the trust dynamics of MANETs, a complex Bayesian network may be constructed from these three nodes.

3.Results and Conclusion Build a MANET with the proactive demand affirmation routing protocol, and then use GloMoSim to enable peer-to-peer communication within the ad hoc network. The gateway is checked without the need of a central administration before selecting an intergateway link. Send the client (the car node) to the gateway first, and if you obtain an acknowledgement and can identify it nearby, send the vehicle node a data request and receive an acknowledgement attached to a routing table or register. Messages of request CV REQ GW are broadcast to all gateways within the client mobile's or client vehicle's hearing range (CV). When a request is made, the gateway nearest to the client answers and chooses to operate as the internet portal until it becomes overloaded, at which time it sends an acknowledgement message to the requesting client (GW ACK). When the client vehicle is overloaded, the closest gateway is selected as the ideal gateway to service it. Next CV sends a message with the data request CV REQ DATA over the specified gateway. The cloud sends the ACK DATA message to tell the requesting CV whether the requested data is accessible or not. When the client vehicle is ready to receive data as shown in Figure 4,5,6.

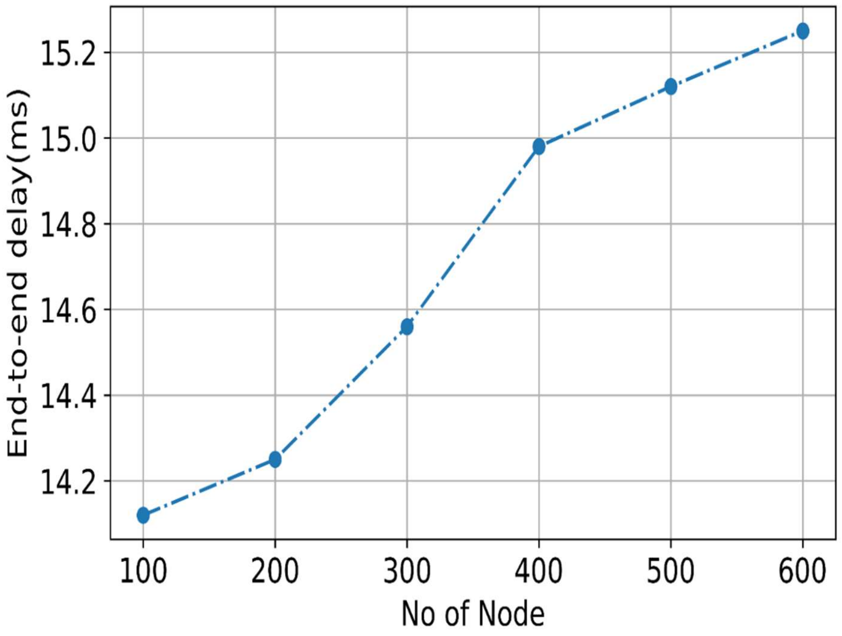

Fig. 4 Network speed vs no of node#throughputtrp=(processing_time + inspection_time + move_time + queue_time)/10network end to end delay vs no of nodedely=Length of packets /Bandwidth

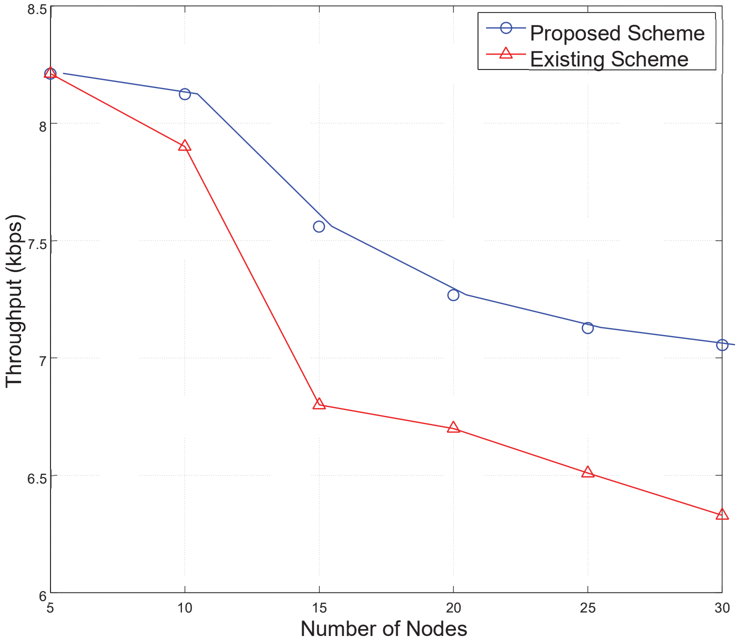

Figure 5. packet delivery ratio vs no of node (packets between sender and resiver)acket delivery ratio =recived pacet/send packets

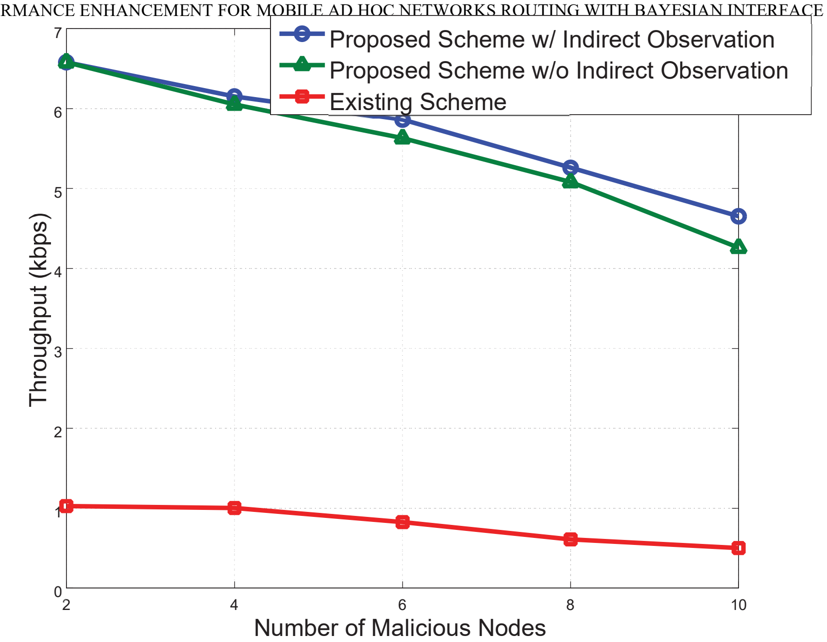

Figure 6 : Relationship between Throughput and Node Velocity

4.Reference

[1] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in *IEEE ICC '08*, (Beijin, CHINA), May 2008.

[2] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trustbased multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 387–399, May 2009.

[3] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM SASN'04*, (Washington, D.C., USA), Oct. 2004.

[4] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM'08*, (Phoenix, AZ, USA), Mar. 2008.

[5] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, H. Tang, and P. Mason, "Trust establishment in cooperative wireless networks," in *Proc. IEEE Milcom'10*, (San Jose, CA, USA), Nov. 2010.

[6] S. Jana, K. Zeng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," in *Proc. IEEE INFOCOM'12*, (Orlando, FL, USA), Mar. 2012.

[7] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3064 –3073, Sept. 2011.

[8] L. Wasserman, *All of Statistics: A Concise Course in Statistical Inference*.

Springer, 2004.

[9] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability, Second Edition*. Athena Scientific, 2008.

[10] Y. Beghriche, V. Toubiana, and H. Labiod, “A bayesian filter to detect misbehaving nodes in manets,” in *Proc. NTMS’08*, (Tangier, Morocco), Nov. 2008.

[11] B. Elizabeth, R. Aaishwarya, P. Kiruthika, M. Shrada, A. Prakash, and V. Uthariaraj, “Bayesian based confidence model for trust inference in manets,” in *Proc. IEEE ICRTIT’11*, (Chennai, Tamil Nadu, India), Jun. 2011.

[12] M. Mehdi, N. Bouguila, and J. Bentahar, “A QoS-based trust approach for service selection and composition via bayesian networks,” in *Proc. IEEE ICWS’13*, (Santa Clara, CA, USA), Jun. 2013.

[13] S. Corson and J. Macker, “Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations,” *IETF RFC 2501*, Jan. 1999.

[14] J. Chapin and V. W. Chan, “The next 10 years of DoD wireless networking research,” in *Proc. IEEE Milcom’11*, (Baltimore, MD, USA), Nov. 2011.

[15] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Securing mobile ad hoc networks with certificateless public keys,” *IEEE Trans. Dependable and Secure Computing*, vol. 3, pp. 386–399, Oct.–Dec. 2006.

[16] Y. Fang, X. Zhu, and Y. Zhang, “Securing resource-constrained wireless ad hoc networks,” *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, 2009.

[17] W. Lou, W. Liu, Y. Zhang, and Y. Fang, “SPREAD: improving network security by multipath routing in mobile ad hoc networks,” *ACM Wireless Networks*, vol. 15, no. 3, pp. 279–294, Mar. 2009.

[18] R. Zhang, Y. Zhang, and Y. Fang, “AOS: An anonymous overlay system for mobile ad hoc networks,” *ACM Wireless Networks*, vol. 17, no. 4, pp. 843–859, May 2011.

[19] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, “Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches,” in *Proc. 1st Int’l Workshop on Wireless information Systems*, (Ciudad Real, Spain), Apr. 2002.

[20] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” *IEEE Wireless Comm.*, vol. 11, pp. 48–60, Feb. 2004.

[21] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, “A survey on trust and reputation management systems in wireless communications,” *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[22] H. Kobayashi, B. L. Mark, and W. Turin, *Probability, Random Processes, and Statistical Analysis*. Cambridge University Press, 2011.

[23] Y. Owada, T. Maeno, and H. Imai, "OLSRv2 implementation and performance evaluation with link layer feedback," in *Proc. ACM IWCMC'07*, (Honolulu, Hawaii, USA), Aug. 2007.

[24] C. Dearlove, T. Clausen, and P. Jacquet, "Link metrics for olsrv2," *IETF draftdearlove-olsrv2-metrics-05*, Jun. 2010.

[25] "Trust platform module." website: http://www.trustedcomputinggroup.org/.