iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** X **Month of publication:** October 2022

DOI: https://doi.org/10.22214/ijraset.2022.46949

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Finding Optimal Path and Privacy Preserving for Wireless Network

Manasi Kiranagi[1], Devika Dhoble[2], Madeeha Tahoor[3], Dr. Rekha Patil[4]
Department Of Computer Science &Engineering, PDA College of Engineering, Kalaburagi, India

Abstract: Privacy-preserving routing protocols in wireless networks frequently utilize additional artificial traffic to hide the source-destination identities of the communicating pair. Usually, the addition of artificial traffic is done heuristically with no guarantees that the transmission cost, latency, etc., are optimized in every network topology. We explicitly examine the privacy-utility trade-off problem for wireless networks and develop a novel privacy-preserving routing algorithm called Optimal Privacy Enhancing Routing Algorithm (OPERA). OPERA uses a statistical decision-making framework to optimize the privacy of the routing protocol given a utility (or cost) constraint. We consider global adversaries with both Lossless and lossy observations that use the Bayesian maximum-a-posteriori (MAP) estimation strategy. We formulate the privacy-utility trade-off problem as a linear program which can be efficiently solved.

I. INTRODUCTION

Traffic analysis attacks are a serious threat to the privacy of users in a communication system. The analysis attacks can be used to infer sensitive contextual information, source-destination identities from observed traffic patterns. More worryingly, they are easily executed without raising suspicions in a multi hop wireless network where the node transmissions can be passively observed. Hence, extensive research efforts have been invested in mitigating traffic analysis attacks in wireless networks. Typical traffic analysis techniques exploit features such as packet timings, sizes or counts to correlate traffic patterns and compromise user privacy. Three common approaches to mitigate analysis attempts are to: (i) change the physical appearance of each packet at every hop via hop-by-hop encryptions (ii) introduce transmission delays at each hop to de-correlate traffic flows, or (iii) introduce dummy traffic to obfuscate traffic patterns. The first two approaches may not be desirable for low-cost or battery-powered wireless networks, e.g., wireless sensor networks as (i) the low-cost nodes may not be able to afford using the computationally expensive encryptions at each hop, and (ii) introducing delays at the intermediate nodes may not be effective when there is little traffic in the network. Therefore, we use the dummy traffic approach to provide privacy by lowering the adversary's detection rates in a wireless network. Specifically, considered an adversary that uses the optimal maximum-a-posteriori (MAP) estimation strategy ions in the entire network was considered The periodic collection and source simulation techniques for providing source location privacy and the backbone flooding and sink simulation techniques for receiver location privacy the authors designed a packet transmission protocol based on random route generation and dummy packet transmissions that is secure against internal adversaries who can view the routing tables of the nodes the authors proposed that the destination node randomly forwards some of the packets it receives to a randomly selected neighbor node located M hops away from the destination. A heuristic probabilistic routing algorithm was also used against the global adversary. Lastly, the work proposed a cloud-based scheme for enhancing the source node privacy and used symmetric-key cryptography operations and trapdoor techniques to develop a secure and privacy-preserving communication protocol.

II. RELATED WORK

A. *J. Deng, R. Han, and S. Mishra, "Countermeasures against trafficanalysis attacks in wireless sensor networks," in Proc. Int. Conf. Security and Privacy for Emerging Areas in Commun. Networks, pp. 113–126, 2005.*

In this paper Securing surveillance wireless sensor networks (WSNs) in hostile environments such as borders, perimeters and battlefields during Base Station (BS) failure is challenging. Surveillance WSNs are highly vulnerable to BS failure. The attackers can render the network useless by only destroying the BS as the needed efforts to destroy the BS is much less than that is needed to destroy the network. This attack scenario will give the attackers the best chance to compromise many legitimate nodes. SurvSec security architecture provides methodologies for choosing and changing the security managers of the surveillance WSN. SurvSec has three components: (1) Sensor nodes serve as Security Managers, (2) Data Storage System, (3) Data Recovery System. Furthermore, both the frame format of the stored data is carefully built and the security threats are encoded to allow minimum overheads for SurvSec security architecture. In this paper, they provide detailed specifications of SurvSec security architecture.

We evaluate our designed security architecture for reliable network recovery from BS failure. Our evaluation shows that the proposed new security architecture can meet all the desired specifications and our analysis shows that the provided Security Managers are capable of network recovery from BS failure.

B. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks

In this paper for sensor networks deployed to monitor and report real events, event source anonymity is an attractive and critical security property, which unfortunately is also very difficult and expensive to achieve. They propose a scheme called *FitProbRate*, which realizes statistically strong source anonymity for sensor networks. They demonstrate the robustness of our scheme under various statistical tests that might be employed by the attacker to detect real events. Their analysis and simulation results show that their scheme, besides providing source anonymity, can significantly reduce real event reporting latency compared to two baseline schemes.

They propose a *dynamic mean* scheme which has better performance under high real message rates. Simulation results show that the dynamic mean scheme is capable of increasing the attacker's false positive rate and decreasing the attacker's Bayesian detection rate significantly even under high-rate continuous real messages.

C. J. Y. Koh, J. Teo, D. Leong, and W.-C. Wong, "Reliable privacy preserving communications for wireless ad hoc networks," in Proc.

In this paper Device-to-Device (D2D) communication presents a new paradigm in mobile networking to facilitate data exchange between physically proximate devices. The development of D2D is driven by mobile operators to harvest short range communications for improving network performance and supporting proximity-based services. In this article, they investigated two fundamental and interrelated aspects of D2D communication. By the primary goal of our work is to equip researchers and developers with a better understanding of the underlying problems and the potential solutions for D2D security and privacy. To inspire follow-up research to the best of thier knowledge, this is the first comprehensive review to address the fundamental security and privacy issues in D2D communication. Index Terms Device-to-Device (D2D) Communication, Security, Privacy.

D. P. Zhang, C. Lin, Y. Jiang, P. Lee, and J. Luis, "ANOC: Anonymous network-coding-based communication with efficient cooperation," IEEE J. Sel. Areas Communication

In this paper Practical wireless network coding is a promising technique that can enhance the throughput of wireless networks. However, such a technique also bears a serious security drawback: it breaks the current privacy-preserving protocols, since their operations conflict each other.

They apply the idea of cooperative networking and design a novel anonymity scheme named ANOC, which can function in network-coding-based wireless mesh networks. ANOC is built upon the classic Onion Routing protocol, and resolves its conflict with network coding by introducing efficient cooperation among relay nodes. Using ANOC, they can perform network coding to achieve a higher throughput, while still preserving user privacy in wireless mesh networks. They formally show how ANOC achieves the property of relationship anonymity, and conduct extensive experiments via nsclick to demonstrate its feasibility and efficiency when integrated with network coding.

E. H. Sheen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs

In this paper Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. To offer high anonymity protection at a low cost, we propose an Anonymous Location- based Efficient Routing proTocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers.

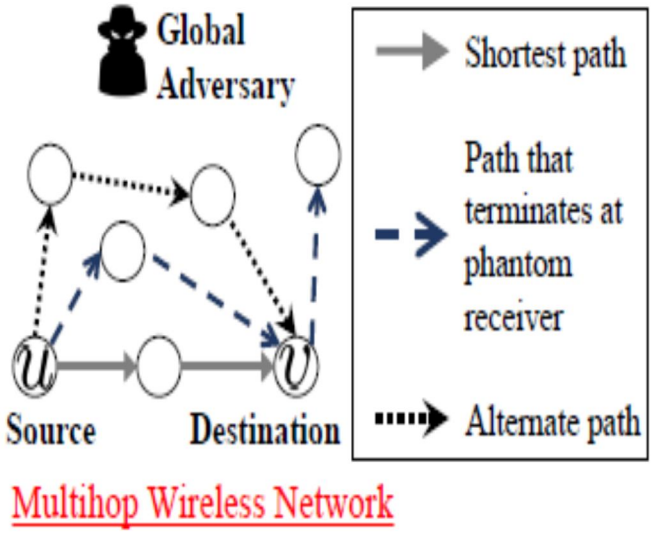
Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter inter-section and timing attacks. Experimental results show that ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

III. PROPOSED WORK

1) We focus on hiding the source-destination identities of each communication where a global adversary is able to observe node transmissions from the entire network.
2) Our challenge is to decide how to probabilistically route the packets from the source to the destination nodes via carefully chosen receiver nodes to preserve privacy.
3) Even though it is desirable to maximize the amount of privacy for each communicating party, this would usually require a flooding based solution which is undesirable due to its high network resource consumption.
4) Hence, we present the Optimal Privacy Enhancing Routing Algorithm (OPERA) which uses a statistical decision-making framework to characterize different network scenarios and select the optimal path distribution that strikes a balance between the privacy and utility of the routing protocol given some privacy budge. Additional dummy traffic may also be used to extend the routing path to include additional receiver nodes.

IV. SYSTEM ARCHITECTURE



Multihop Wireless Network

We consider the scenario where a source node u wants to send packets to a single destination node v in a static wireless network. The source node uses a dynamic source routing and specifies a routing path from itself to the destination. Due to the wireless broadcast nature of the network, when a node transmits, all its one-hop neighbors are able to receive the transmission. Next, we introduce the graph notations used in the paper: a. Let the wireless network be modeled as a connected hyper graph G = (V, H) where V is the set of nodes and H is the set of (directed) hyper arcs. A hyper arc h = (s, R) represents a source-receivers pair where s ∈ V is the source node and R ⊆ V is a non-empty set of receiver nodes adjacent to s. b. Let w, (u, v) represent the source-destination pair, where u ∈ V, v ∈ V are the source and destination nodes respectively. c. Let x = (h1, h2 . . .) be the actual transmission path comprising the distinct hyper arcs hi and the source node of hi+1 must be a receiver node of hi . Let y be the observed path where y is a sub vector of x. An observer may not necessarily observe all the hyper arc transmissions in x as some of them may be erased i.e., lossy observations. The ordering of the observed transmissions, however, remains unchanged d. Let X represent the set of all possible paths x in the network and let X w be the set of all paths x = (h1, h2 . . .) that serve the source-destination pair w = (u, v), i.e., h1 = (u, R) and there exists an h = (s, R) ∈ x such that v ∈ R. Let Y represent the set of all possible observations y. e. Let ch ≥ 0 represent the cost e.g., transmission cost for using hyper arc h. Definition 1 Routing Protocol. Given a network graph G, a probabilistic source-routing protocol selects a path x ∈ X w according to a path distribution p (x|w) for a given source destination pair w ∈ V2 . Optimized Probabilistic Routing: We focus on protecting the privacy of the source-destination identities by designing a probabilistic privacy-preserving routing protocol to minimize the probability of an adversary correctly guessing the source-destination identities. In addition, the routing scheme should consider the adversary's observation model p (y|x) while computing a routing path distribution p (x|w) that serves the source-destination pair w.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

V. IMPLEMENTATION

Network simulation (NS) is one of the types of simulation, which is used to simulate the networks such as in MANETs, VANETs, etc. It provides simulation for routing and multicast protocols for both wired and wireless networks. NS is licensed for use under version 2 of the GNU (General Public License) and is popularly known as **NS2**. It is an object-oriented, discrete event-driven simulator written in C++ and Otcl /Tcl.

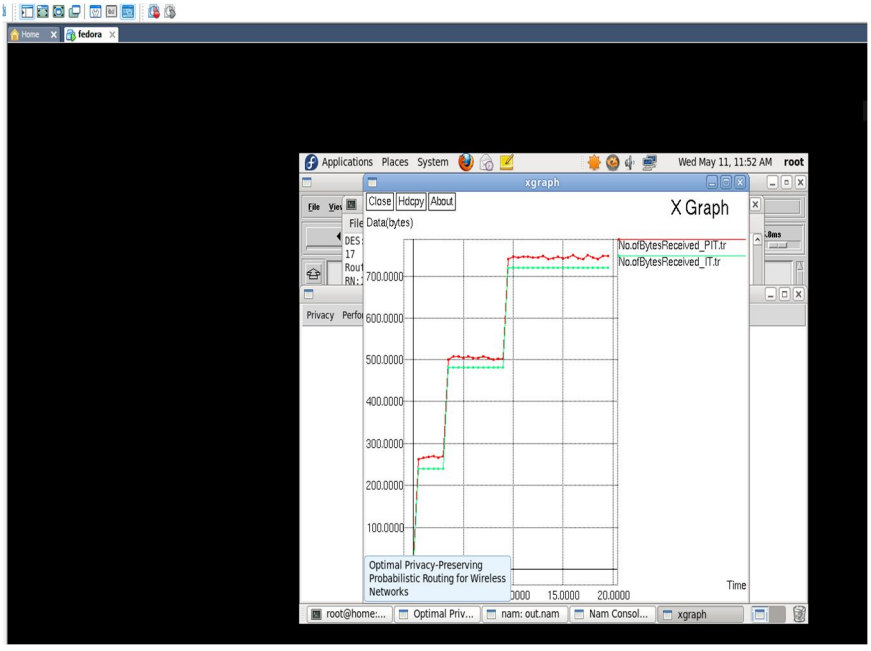
Privacy-preserving routing protocols, the routing protocol i.e., Dynamic Source routing protocol: it allows a sender of a packet to partially or completely specify the route the packet that takes through the network

A. Node Initialization Phase

1) *Network Setup:* Network configuration is the process of setting a networks controls, flow and operation to support the network communication of an organization and/or network owner. This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components to find out the optimal path to avoid from hackers.
2) *Pre Processing:* Pre processing is the process of transforming raw data into an understandable format. It is also an important step in data as we cannot work with raw data. The quality of the data should be checked.
3) *Privacy:* Security is generally perceived as a technical issue, while data privacy and protection is regarded as an issue relating to data access and protecting data from getting into the wrong hands. Simply put, security is a technical way of implementing data privacy.
4) *Performance Analysis:* For the proposed framework, we utilize the accompanying particular estimations to assess its execution : The measurement of these things is not in term of number of packets sent to the receiver node in a given time , End-to-End Delay's is also main issue analyzed , Data should not dropped from the network's.

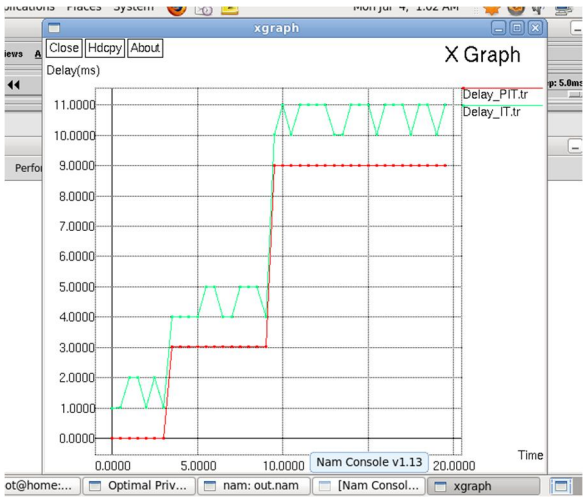
VI. RESULT

A. NO.OF Bytes Graph



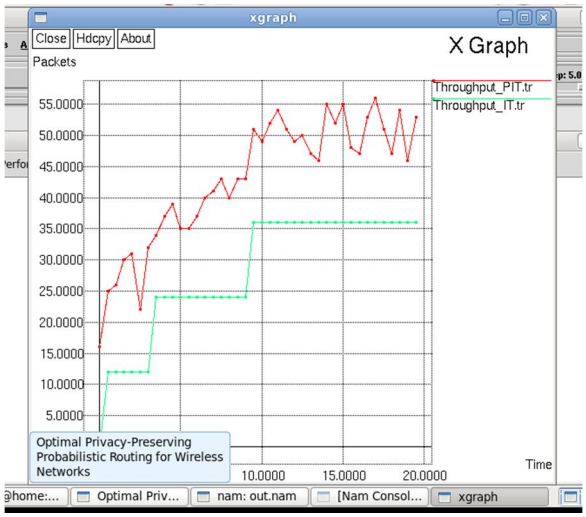
In most computer systems, a byte is a unit of data that is eight binary digits long. A byte is the unit most computers use to represent a character such as a letter, number or typographic symbol. Each byte can hold a string of bits that need to be used in a larger unit for application purposes. As an example, a stream of bits can constitute a visual image for a program that displays images. Another example is a string of bits that constitute the machine code of a computer program.

B. Delay Graph



Network latency, sometimes called lag, is the term used to describe delays in communication over a network. Latency meaning in networking is best thought of as the amount of time it takes for a packet of data to be captured, transmitted, processed through multiple devices, then received at its destination and decoded. When delays in transmission are small, it's referred to as a low-latency network (desirable) and longer delays are called a high-latency network (not so desirable). Long delays that occur in high-latency networks create bottlenecks in communication. In the worst cases, it's like traffic on a four-lane highway trying to merge into a single lane. High latency decreases communication bandwidth, and can be temporary or permanent, depending on the source of the delays. Latency is measured in milliseconds, or during speed tests, it's referred to as a ping rate. The lower the ping rate the better the performance. A ping rate of less than 100ms is considered acceptable but for optimal performance, latency in the range of 30-40ms is desirable. Obviously, zero to low latency in communication is what we all want. However, standard latency for a network is explained slightly differently in various contexts, and latency issues also vary from one network to another.

C. Throughput Graph



Network throughput (or just throughput, when in context) refers to the rate of successful message delivery over a communication channel, such as Ethernet or packet radio, in a communication network. The data that these messages contain may be delivered over physical or logical links, or through network nodes. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot. The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. [1]

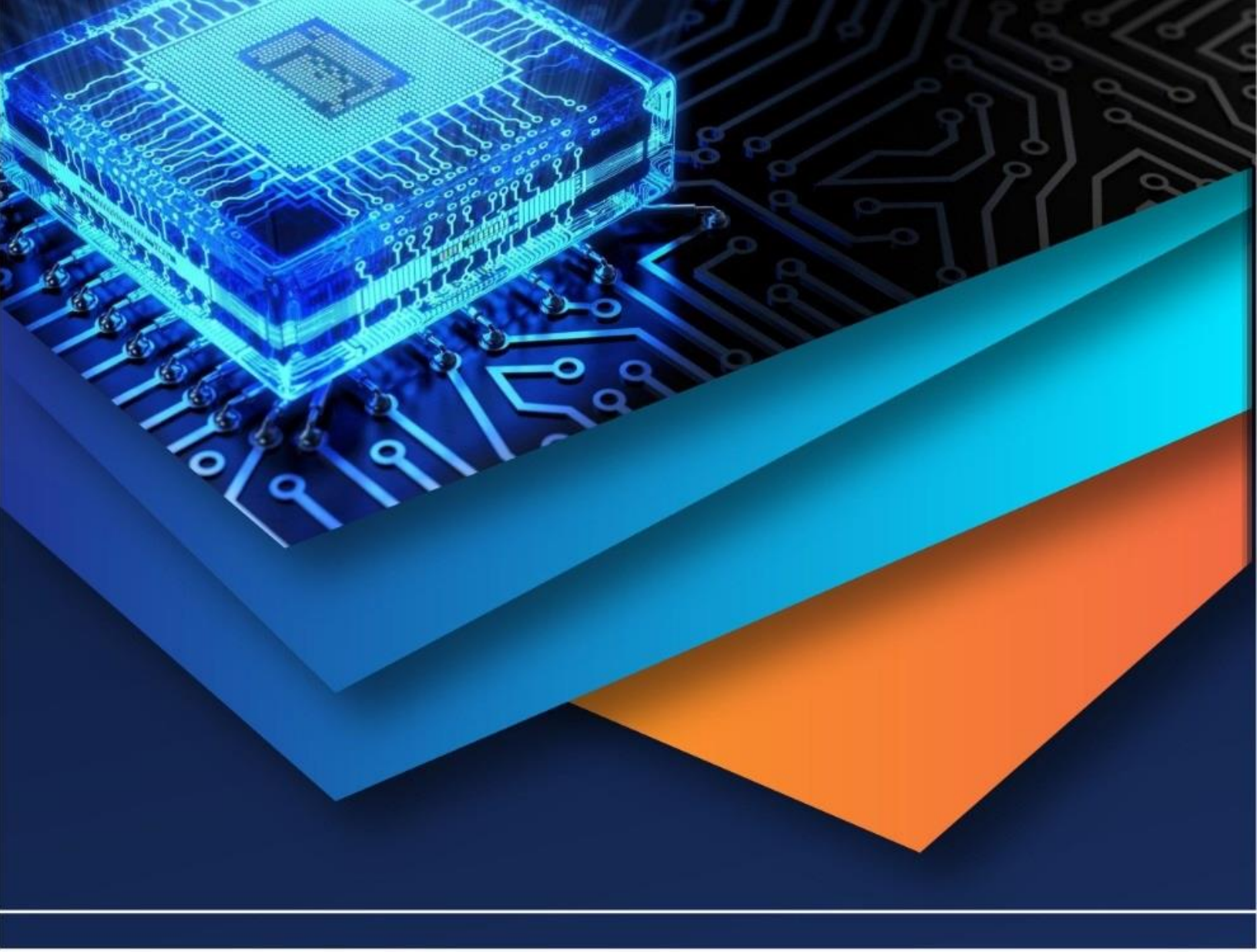
Throughput is essentially synonymous to digital bandwidth consumption; it can be determined numerically by applying the queuing theory, where the load in packets per time unit is denoted as the arrival rate (λ), and the drop in packets per unit time is denoted as the departure rate (μ). The throughput of a communication system may be affected by various factors, including the limitations of the underlying analog physical medium, available processing power of the system components, end-user behavior, etc. When taking various protocol overheads into account, the useful rate of the data transfer can be significantly lower than the maximum achievable throughput; the useful part is usually referred to as good put.

VII. CONCLUSION

We have developed a statistical decision-making framework to optimally solve the privacy-preserving routing problem in wireless networks given some utility constraints assuming a powerful global adversary that uses the optimal maximum-a-posteriori (MAP) estimation strategy. We also showed via simulations that our approach is significantly better than the Uniform and Greedy heuristics, a baseline scheme, and the mutual information minimization scheme. For future work, it would be interesting to study the privacy-utility trade-off problem for mobile networks and to provide stricter privacy constraints for the communicating parties.

REFERENCES

[1] J. Deng, R. Han, and S. Mishra, “Countermeasures against trafficanalysis attacks in wireless sensor networks,” in Proc. Int. Conf. Security and Privacy for Emerging Areas in Commun. Networks, pp. 113–126,2005.
[2] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks
[3] J. Y. Koh, J. Teo, D. Leong, and W.-C. Wong, “Reliable privacypreserving communications for wireless ad hoc networks,” in Proc.
[4] P. Zhang, C. Lin, Y. Jiang, P. Lee, and J. Lui, “ANOC: Anonymous network-coding-based communication with efficient cooperation,” IEEE J. Sel. Areas Communication
[5] H. Shen and L. Zhao, “ALERT: An anonymous location-based efficient routing protocol in MANETs
[6] M. Conti, J. Willemsen, and B. Crispo, “Providing source location privacy in wireless sensor networks: A survey,” IEEE Commun. Surveys.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY