RESEARCH ARTICLE OPEN ACCESS

# Analyze and Detect Packet Loss for Data Transmission in WSN

*Miriam Lakde, **Prof. Vaibhav Deshpande
**(Department of Computer Science & Engineering St. Vincent Pallotti College of Engineering & Technology Nagpur, India, miriam.lakde@gmail.com)*
*** (Department of Computer Engineering St. Vincent Pallotti College of Engineering & Technology Nagpur, India, vabartday@gmail.com)*

**ABSTRACT**
An emerging technology is Wireless Sensor Network where sensors are deployed at extreme geographical locations where human intervention is not possible. The data transferred through the sensor nodes are majorly used in crucial decision making process. Since WSN is a wireless infrastructure it tempts the attackers to tamper/misuse the data. Privacy-preserving routing is important for some ad hoc networks that require stronger privacy protection. Hence a routing protocol to achieve total unobservability by anonymous key establishment using secret session keys and group signature is used. The unobservable routing protocol is divided into two main phases. First phases define an anonymous key establishment process to construct secret session keys. Second phase consist of unobservable route discovery process to find appropriate as well as secure route to the destination. A node establishes a key with its direct neighbour and uses the same key to encrypt the packet before transferring.

***Keywords:*** Security, Sensor Networks, Privacy, MANET

## I. INTRODUCTION

Wireless Sensor Network consists of sensor nodes grouped into one network. They are placed at different geographical locations and data can be collected with ease, the main reason of WSN growing rapidly is the sensor nodes among the network that do not require physical infrastructure and can be placed at extreme environmental conditional where human interventions are not possible.

The main concept acting as a pillar behind mobile ad hoc networking is multi-hop relaying, which indirectly refers finding alternate solutions for message transferring if destinations are unreachable. Special kind of Wireless sensor networks that work in decentralized environments are MANETs where in every node is capable of forwarding the data to its neighbor within the frequency range which eventually transfer the data to the specified destination. The data transferred play an important role important in terms of decision making processes if they belong to large scales networks. Hence the data needs to be transferred with utmost security. In comparison to Wired networks, Wireless nodes are more prone to attacks such as DOS, wormhole, Tunneling, Sybil, Traffic analysis, all these attacks lead to Packet drops within the network, which indirectly effects the packet delivery ratio, more energy consumption and less throughput. In contrast, the attacker only needs a selected transceiver which can analyse the data silently via traffic analysis and receive wireless signal without being detected.

All previous methods first identifies the wormhole attack and then find appropriate solutions to remove them from the network, which is indirectly time as well as energy consuming process. A method that selects appropriate route "avoiding" rather than "identifying" the wormhole attack resulting in low over head as well as low cost is used.

The summarization of the paper is as follows. In Section II review of work related to packet loss has been discussed. In Section III Mechanisms and solutions to avoid packet drop is explained. Section IV describes about the Experimental setup and results. Section V concludes the paper with the conclusion and future work

## II. RELATED WORK DONE

In Hop-count analysis scheme for avoiding wormhole attacks in MANET instead of detecting wormholes [3] from the role of administrators as in previous methods, they implement a new protocol, MHA, using a hop-count analysis from the viewpoint of users without any special environment assumptions. They provide four simulations to show the proposed scheme has high efficiency and very good performance with low overhead. In addition, this scheme does not require additional hardware or impractical assumptions of the networks. Hence, it can be directly used in MANET. The disadvantage of this system is that the dynamic information of the packets could still be modified.

Provenance- Aware Storage systems: is a survey of multi-hop [5] sensor network by using the data provenance scheme the BS can trace the source and forwarding path of an individual data packet. For each packet Provenance must be recorded but there is an important challenge arises due to the heavy storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance scheme with low overhead.

Unobservable Privacy-Preserving Routing in MANET is an efficient privacy-preserving routing [7] achieving content unobservability by employing anonymous key establishment based on group signature. The disadvantage of this system is that they have only focused on security and full privacy preserved routing in mobile ad hoc networks have not been addressed.

Secure Data Aggregation in Wireless Sensor Networks, this work deals with attacks against the synopsis [8] diffusion. This aggregation work presents a lightweight verification algorithm to make verification at the BS. The several synopses generated should be verified independently by the verification protocol at three phases. The phases are query dissemination phase, aggregation phase and the verification phase. In the first phase called query dissemination phase, the BS broadcasts the aggregation name to compute a random seed. In second phase called the aggregation phase, each node computes a sub aggregate value based on the local value and the synopses of its children. The node also randomly selects a set of MACs. Finally, in the third phase called verification phase, the BS computes the final synopses using the messages from its child nodes and verifies the received MACs.

Anonymizing Geographic Routing for Preserving Location Privacy Using Unlink ability and Unobservability, it describes a framework supporting anonymous location-based [9] routing in certain types of suspicious MANETS. But the framework has not been extended to analytical model which captures the loss in node privacy due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks, it describes about the introduction of efficient mechanisms for provenance verification and reconstruction [11] at the base station. In addition, they extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The disadvantage of this system is that the packet dropped by the malicious nodes through various attacks cannot be distinguished

Querying and Maintenance of Network Provenance at Internet-Scale, It describes the history and sub part [14] of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is also does not address security concerns and is specific to some network use cases.

## III. PROPOSED METHODOLOGIES

The main factor that affects the packet loss ratio is Unobservability and security within the network to avoid unauthorized access of data /packet while transferring to other nodes. The unobservable routing protocol [12] is executed in two phases.

Anonymous trust establishment

Unobservable route discovery

The unobservable routing protocol is implemented using two scenarios:

**Scenario I:** Attack by malicious node within the network causing packet drop

**Step 1:** Deployment of nodes

**Step 2:** Topology Creation

**Step 3:** Communication among nodes

**Step 4:** Path selection

**Step 5:** Data transfer among selected nodes

**Step 6:** Dropping of packets by malicious node from the nearest node

**Scenario II:** Selection of secure route to transfer data from source to destination without attack (Packet drops) is identified using the unobservable routing protocol.

It will check each node by communicating with the other, and then decide secure path for data transfer from source to destination.

## IV. EXPERIMENTAL RESULTS

### *A. Experimental Setup*

For attacks some node models, process models, & packet models are created into the simulation network, some predefined node models from library are also used. The details of models with their technical parameters are as follows

- Total Nodes = 50
- Infected node=11
- Packet size = 1024 bits constant
- Applying protocol=DSDV

The simulation of the proposed scheme is performed in Network Simulator2 (NS2) to prove practical efficiency of the scheme, the physical parameter considerations are same as taken in mathematical modelling

**Scenario 1:** Attacks causing packet loss

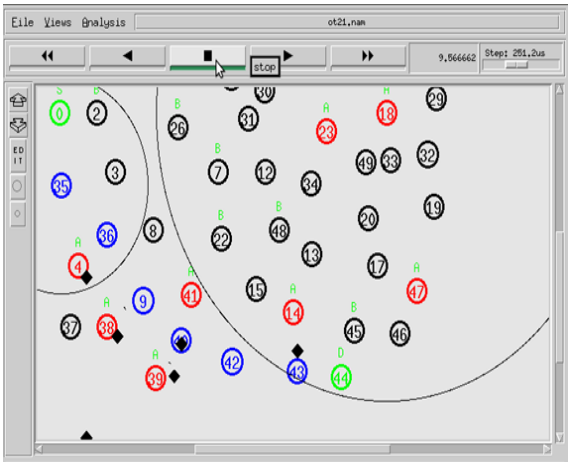


**Fig 1.** Attackers dropping packet from its nearing nodes

**Scenario 2:** Selection of secure path

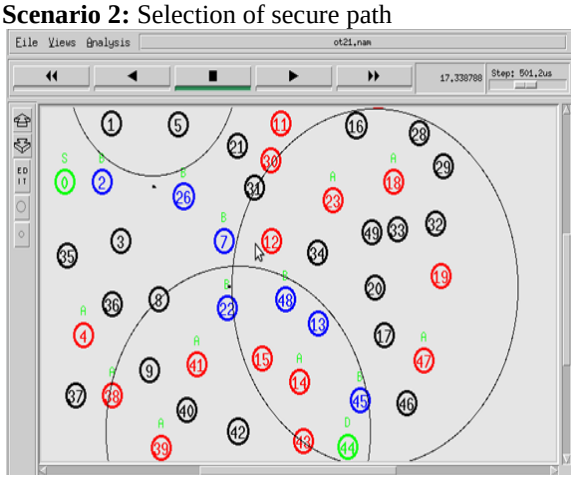


**Fig 2.** Secure path selected without packet loss

***B. Result***

Simulations are carried out in NS2 and results are obtained.

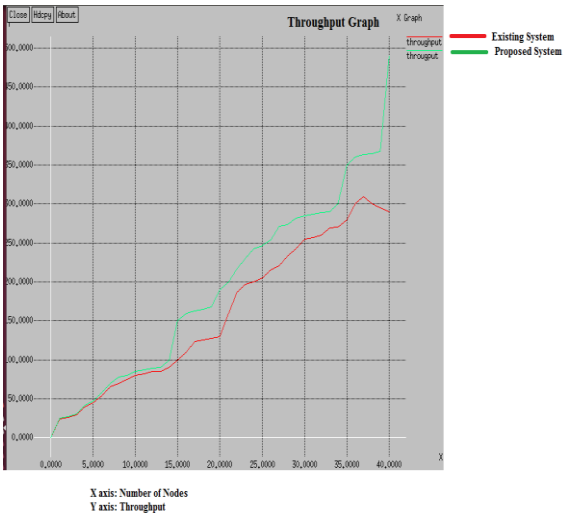


**Fig 3.** Throughput comparison before and after packet loss

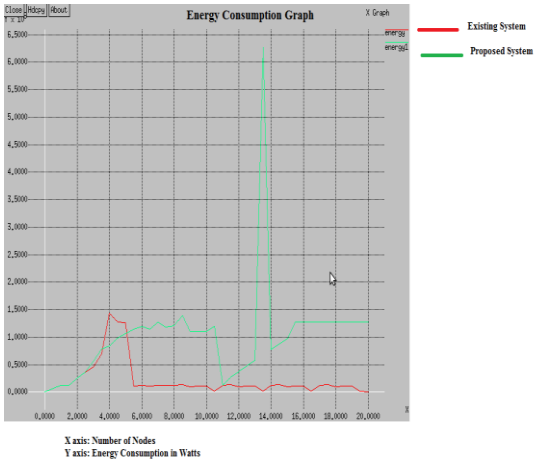


**Fig 4.** Energy comparison before and after packet loss

## V. CONCLUSION AND FUTURE SCOPE

In this paper an analysis of different packet loss system is observed, the main cause for packet drop is lack of security measures while data transmission in Wireless network. In the research, a routing protocol to achieve total unobservability considering appropriate security measures along with provenanceis used to avoid packet loss by securely transmitting data within the wireless network. From the experiment an effective result for increase in packet delivery ratio and less packet loss during transmission has been observed as compare to other systems. Hence a conclusion can be made that system is more effective in securely transmitting data with improved data throughput as well as increase in Packet delivery ratio due to less packet loss.

In future, this project work can be extended to recover data loss during the packet loss, also a malicious packet dropping detection technique can be designed that can effectively detects the packet dropping attack in any environment while keeping generated over heads minimal.

## REFERENCES

[1]. Vijay Bhuse, Ajay Gupta, and Leszek Lilien. “DPDSN: Detection of packet-dropping attack for wireless sensor networks”, *IEEE 2005*.

[2]. W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, “Efficient Querying and Maintenance of Network Provenance at Internet- Scale ,”*Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 615-626, 2010. 2011.*

[3]. Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo. “A Hop-Count Analysis

Scheme for Avoiding Wormhole Attacks" in MANET", *Sensors 9.6 (2009): 5022-5039*

[4]. R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," *Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.*

[5]. K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," *Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.*

[6]. T.Sathyamoorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini, "A simple and effective scheme to find malicious node in wireless sensor network", *in IJRET: International Journal of Research in Engineering and Technology Volume: 03 Issue: 02, Feb-2014, eISSN: 2319-1163, pISSN: 2321-7308.*

[7]. P.Thamizharasi and D.Vinoth, "Unobservable Privacy-Preserving Routing In MANET", in *IJESE, ISSN: 2319–6378, Volume-2, Issue-3, January 2013.*

[8]. S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," *IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.*

[9]. Venkatesan R, K. G. S., and R. Remya Resmi. "Anonymizing geographic routing for preserving location privacy using unlinkability and unobservability." *International Journal* 4.3 (2014).

[10]. Duche, Ravindra Navanath, and Nisha P. Sarwade. "Sensor node failure detection based on round trip delay and paths in WSNs." *IEEE Sensors Journal 14.2 (2014): 455-464.*

[11]. Salmin Sultana, Gabriel Ghinita, Elisa Bertino, and Mohamed Shehab, " A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks journal of latex class files, vol. 6, no. 1, January 2007" *IEEE transactions on depedable and secure computing. pp 256 – 269, 2015.*

[12]. Shylaja, B. N., and S. Devaraja. "Assured Scheme for Investigating Provenance Falsification & Packet loss Attacks in Wireless Sensor Networks." *(2016).*

[13]. Edemacu, Kennedy, Martin Euku, and Richard Ssekibuule. "Packet drop attack detection techniques in wireless ad hoc networks: a review." *arXiv preprint arXiv:1410.2023*

[14]. Zhou, Wenchao, et al. "Efficient querying and maintenance of network provenance at internet-scale." *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data. ACM, 2010.*

[15]. Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks" in MANET", *Sensors 9.6 (2009): 5022-5039.*

[16]. Patil, Vaishali, Priyanka Fulare, and Nitesh Ghodichor. "An Unobservable Secure Routing Protocol with Wormhole Attack Prevention for Mobile Ad-Hoc Network." (2014) *International Journal of Current Engineering and Technology E- ISSN 2277 – 4106, P-ISSN 2347 – 5161.*

[17]. Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, NehaGarg, "Analysis of denial of service (dos) attacks in wireless sensor networks", *in IJRET: International Journal of Research in Engineering and Technology Volume: 03 Special Issue: 10 NCCOTII 2014, Jun-2014,eISSN: 2319-1163, pISSN: 2321-7308.*

[18]. Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap, "Detection of Wormhole Attack using Hop-count and Time delay Analysis" *International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153*

[19]. Khainwar, Rajpal Singh, Mr Anurag Jain, and Mr Jagdish Prasad Tyagi. "Elimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm." *International Journal of Emerging Technology and Advanced Engineering 1.2 (2011): 40-47.*

[20]. Wang, Chuang, et al. "Catching packet droppers and modifiers in wireless sensor networks." *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, 2009.*

[21]. S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," *in Proc. of ICDCS Workshops, 2011, pp. 332–338.*