

# Reducing the Delay Using IDS and Improving the Speed of Data Transmission in Collaborative Contact Based Watchdog System

B.Vinoth<sup>1</sup>, L.S.Usharani<sup>2</sup> & G.Gandhimathi<sup>3</sup>

<sup>1</sup>M.tech Scholar, <sup>2,3</sup>Asst Prof

School of Engineering and Technology, Periyar Maniammai University, Thanjavur, India

**Abstract:** Mobile Adhoc networks are playing major role in data transmission and other communication systems. Collaborative contact based watchdog system is one of the best ways to detect selfish nodes. In this method it has some disadvantages, like delay and packet loss. Selfish node detection is more important in communication systems. Using of IDS (Intrusion detection system) is more helpful to reduce the delay of data transmission. It detects the selfish nodes before the communication will start, the path also changed before it. So the Time delay and packet loss will reduce gradually. It helps to increasing the speed of data transmission.

**Index Terms** – Mobile Adhoc Networks, IDS (Intrusion Detection System), Selfish nodes.

## 1. Introduction

Selfish nodes are major factor for delay communication. Network topology changes rapidly and unpredictably over time due to the mobility of the nodes. There arises the need of incorporating the routing functionality into nodes. MANETs are vulnerable to malicious entities that aim to tamper and analyses data and traffic analysis by communication attacking routing protocols. The identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyses data integrity, and more. Depending on the detection methods you choose to deploy, there are several direct and incidental benefits to using an IDS. Understanding what an IDS is, and the functions it provides, is key in determining what type is appropriate to include in a computer security policy.

An ad hoc network is a group of wireless mobile computers (or nodes), in which nodes cooperate by forwarding packets for each other to

allow them to communicate beyond direct wireless transmission range.

## 2. Architecture of IDS System

Intrusion prevention mechanism is one of the major and efficient methods against attacks, but there might be some attacks for which prevention method is not known. Besides preventing the system from some known attacks, intrusion detection system gather necessary information related to attack technique and help in the development of intrusion prevention system. In this proposed intrusion detection system architecture we followed clustering mechanism to build a four level hierarchical network which enhances network scalability to large geographical area and use both anomaly and misuse detection techniques for intrusion detection.

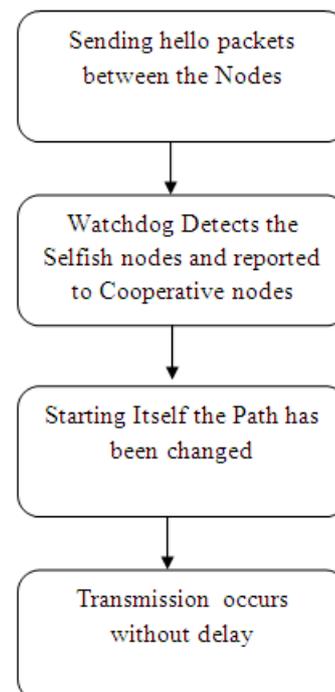


Fig 2.1 Architecture of IDS System

In this Architecture the hello packets were sending at the beginning of the transmission. The watchdog detects the selfish nodes and reported it to cooperative nodes. The cooperative nodes send it to initial node. So at the beginning itself the path has been changed. By this method the delay and packet loss will reduce drastically.

### 3. Watchdog's Detection Technique

Watchdog technique as an effective technique for detecting malicious nodes based on a power aware hierarchical model. This technique overcomes the common problems in the original Watchdog mechanism. The main purpose to present this model is reducing the power consumption as a key factor for increasing the network's lifetime. For this reason, we simulated our model with Tiny-OS simulator and then, compared our results with non hierarchical model to ensure the improvement.

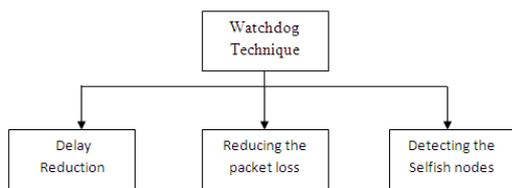


Fig 3.1 Watchdog's

Detection Technique

Watchdog Technique is mostly used for detecting the selfish nodes. It reduces the delay time and the packet loss. The connection between these three activities is reliable. The Selfish node will get reduced means the delay time and packet loss getting reduced. So these are the major relation between these Activities.

### 3.1 Watch Dog and Path Ratter

When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is considered as misbehaving. The path ratter uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets. The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

## 4. Literature survey

S.no	Author and Year of Publication	Title	What is Done	Advantage	Disadvantage
1	Mohammad Saiful Islam Mamun	Hierarchal Design Based Intrusion Detection System For Wireless Adhoc Network	GSM cell concept for intrusion detection architecture.	It is only for GSM	Sometimes it may attack good Nodes
2	Nithya Karthika , Raj Kumar	Survey on Network Based Intrusion Detection System in Manet	scan network packets at the router	Scan process has implemented	It is Explained Only IDS Manet
3.	S. Bansal and M. Baker , 2003.	Observation-based cooperation enforcement in ad hoc networks	Punish Selfish Nodes	It will Punish but	Recover the Node
4.	L. Buttyan and J.-P. Hubaux, 2003.	Stimulating cooperation in self organizing mobile ad hoc networks	Enforce nodes to Cooperate in a Selfish Ad hoc Environment	Nodes Works properly.	It is only for few nodes
5.	Y. Zhang, W. Lee, and Y.-A. Huang, 2003.	Intrusion Detection Techniques for Mobile Wireless Networks	It includes intrusion detection in the security	It is the Firewall of the mobile Nodes.	Not that much Effective

Table 4.1 Literature Survey

## 5. Experimental result

The experimental results are showed, that the packet loss and delay has reduced. Watchdog timers are send information about selfish nodes, and change the path of communication. Initiator, cooperative nodes are gave information about selfish nodes. The transmission speed is improved.

## 6. Future Work

This paper Presents, Improving the speed of data transmission using Intrusion detection System (IDS). In future using of IDS there are so many improvement is possible. The delay and the packet loss have been reduced more. The modification is possible in this paper. There are so many techniques available to speed up the transmission. In this paper IDS technique is used. IDS have so many ways to reduce the packet loss.

## 7. Conclusion

Reducing the delay using IDS and improving the speed of data transmission in collaborative contact based watchdog system is implemented successfully. In this paper the delay and packet loss will reduced drastically. The nodes are transmitted the messages clearly. The selfish nodes are detected before the transmission has started. Watch dog timers detected the selfish nodes and gave the information to initiator. So the delay will reduce and speed of transmission is improved.

## 8. References

- [1] Agrawal.D.P and Qing-An Zeng, Chapter 13, "Wireless & Mobile Systems", Thompson/Brooks Cole, 2003.
- [2] Akyildiz.I.F,Wang.X, and Wang.W, "Wireless mesh networks: a survey," Computer Networks, Vol 47, No 4, March 2005, pp. 445- 487.
- [3] Anderegg.L, Eidenbenz.S, "Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", Proc. ACM Mobicom, pp. 245–259, 2003.
- [4] Brian B. Luu, Barry J. O'Brien, David G. Baran, and Rommie L. Hardy, "A Soldier-Robot Ad Hoc Network" Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07).
- [5] Buchegger.S and Boudec.J.Y.L, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in dynamic ad-hoc

networks," In *Proc. Of MobiHoc*, 2002, pp. 226-236.

- [6] Buttyán.L, Hubaux.J.P, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Technical report No. DSC/2001/001, Swiss Federal Institution of Technology, Lausanne, January 2001. <http://icawww.epfl.ch/hubaux/>.
- [7] Buttyán.L, Hubaux.J.P, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Technical Report No. DSC/2001/046, Swiss Federal Institution of Technology, Lausanne, 31 August 2001. <http://icawww.epfl.ch/hubaux/>. *Analysis*, Vol 23, pp. 29-43, 1996.
- [8] Chen.S and Klara Nahrstedt, "Distributed quality-ofservice routing in ad hoc networks", IEEE Journal on Selected Areas in Communications, vol.17, no. 8, August 1999, pp.1488-1505.
- [9] Christian Tschudin by Why Adhoc Networks, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 - p100.
- [10] Conti.M, Gregori.G, and Maselli.G, "Reliable and efficient forwarding in MANETs," Ad Hoc Networks Journal, Vol 4, No 3, 2006, pp. 398-415.
- [11] Drs. Baruch Awerbuch & Amitabh Mishra Department of Computer Science Johns Hopkins University.