ISSN No: - 2456- 2165

# Defending against Collaborative attacks by Malacious Nodes WSN: CRS-A Approach

[1]P.Sai Akhila,[2]P.L.Sowmya,[3]E.Anna Devi
[1,2]Students,Department of ECE, Sathyabama University
[3]Assistant Professor, Sathyabama University, Chennai

**Abstract:- As a promising event watching and information gathering technique, wireless sensing element network has been wide applied to each military and civilian applications. However, thanks to the dearth of physical protection, sensing element nodes are simply compromised by adversaries, creating WSN liable to varied security threats. One amongst the foremost severe threats is selective forwarding attack, wherever the compromised nodes will maliciously drop a set of forwarding packets to deteriorate the information delivery magnitude relation of the network. During this project, it is proposed that Channel-aware System with adaptive sight ion threshold to detect selective forwarding attacks in WSNs. The CRS-A evaluates the information forwarding behaviors of sensing element nodes, in step with the deviation of the monitored packet loss and also the calculable traditional loss and it optimizes the detection accuracy.**

***Index Terms****—wireless sensing element network, selective forwarding attack, name system, packet dropping, channel-aware, routing.*

## I. INTRODUCTION

As a promising event watching and information gathering technique, wireless sensing element network (WSN) has been wide applied to each military and civilian applications. Several WSNs have deployed in unattended and even hostile environments imbiber type mission-critical tasks, like field of battle intelligence operation and Homeland Security watching. However, thanks to the dearth of physical protection. Sensing element nodes are simply compromised by adversaries, creating WSN liable to varied security threats [1], [2]. One amongst the foremost severe threats is selective forwarding attack, wherever the compromised nodes will maliciously drop a set of forwarding packets to deteriorate the information delivery magnitude relation of the network. It additionally has considerably negative impacts to information integrity, particularly for data-sensitive applications, e.g., health-care and trade watching.

On the opposite hand, since WSNs are typically deployed in open areas (e.g., aboriginal forest), the unstable wireless channel and medium access collision will cause outstanding traditional packet losses. The selective forwarding attacks are hide by the conventional packet losses, complicating the attack detection. Therefore, it's difficult to sight the selective forwarding attacks and improve the network performance. Most of the connected works target watching the packet losses in every transmission link and uninflected the nodes with high packet loss rates from the information forwarding path [3]–[6]. These solutions will improve the information delivery magnitude relation or network turn out however has very little result on police investigation selective forwarding attacks. Since the most challenge of attack detection is to differentiate the malicious drop from traditional packet loss, the conventional packet loss rate of the transmission link ought to be thought of within the forwarding analysis. For instance, a supply node $N_s$ sends 10 packets to the destination node $N_d$ via 2 forwarding nodes $N_a$ and $N_b$, severally. $N_a$ forwards 6 packets to $N_d$, whereas $N_b$ solely forwards 5 packets to $N_d$. Intuitively, sodium behaves higher than $N_b$ throughout the information forwarding. However, if the conventional packet loss rates from Ns to sodium and $N_b$are2 hundredth and five hundredth, severally, A ought to have a better chance to misconduct during this information forwarding. Therefore, we tend to contemplate the deviation between the conventional losses and actual losses because the key issue to sight selective forwarding attacks. However, for the WSNs deployed in hostile environments wherever the wireless channel is unstable, traditional packet loss rate extremely depends on the wireless channel quality that varies spatially and temporally. If it is tend to use a measured or calculable traditional packet loss rate to sight selective forwarding attacks, some innocent nodes could also be incorrectly known as attackers thanks to the time-varied channel condition. For example, if mobile obstacle dead blocks the information transmission of 2sensingnodes, the surprising packet losses could mislead the attack detection. Therefore, a versatile and fault-tolerant analysis technique is crucial to accurately determine the attacks and compromised sensing element nodes [7], [8]. Meanwhile, thanks to the negative impacts of selective forwarding attacks, information delivery magnitude relation of a network becomes the first performance metric for resisting the attacks. though compromised sensing element nodes are often accurately known, they're still on the market candidates to forward information for different sensing element nodes before physically revived or replaced. If a compromised node launches attack with a coffee chance however has sensible channel condition, it may forward more

ISSN No: - 2456- 2165

data packets than a normal node with poor channel condition, in spite of the malicious drops. Therefore, it is of paramount importance to design an attack-tolerant routing scheme to make full use of these nodes or stimulate their cooperation for improving the data delivery ratio. It is proposed that a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detects selective forwarding attacks in WSNs. Specifically, it divides the network lifetime to a sequence of evaluation periods. During each evaluation period, sensor nodes estimate the normal packet loss rates between themselves and their neighboring nodes and adopt the estimated packet loss rates to evaluate the forwarding behaviors of its downstream neighbors along the data forwarding path. The sensor nodes misbehaving in data forwarding are punished with reduced reputation values by CRS-A. Once the reputation value of a sensor node is below an alarm value, it would be identified as a compromised node by CRS-A. Compared to the previous work [10], this has the following enhancements and new contributions.

- It is proposed that CRS-A, which evaluates the forwarding behaviors of sensor nodes by utilizing an adaptive detection threshold. Be theoretically analyzing its performance, it derives an optimal detection threshold for evaluating the forwarding behaviors to optimize the detection accuracy of CRS-A. The optimal detection threshold is determined for each transmission link in a probabilistic way, and can also be adaptive to the time-varied channel condition and the attack probability of the forwarding node.

- It develops a distributed and attack-tolerant data forwarding scheme to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Rather than isolating all the compromised nodes from data forwarding, it jointly considers the time-varied channel condition and attack probabilities of neighboring nodes in choosing forwarding nodes.

- Extensive simulation results demonstrate that the proposed CRS-A with attack-tolerant data forwarding scheme can achieve a high detection accuracy with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.

The remainder of this is organized as follows. Section II reviews the related works. Section III introduces the system model and design goals. The proposed CRS-A is detailed in Section IV and the adaptive detection threshold is determined in Section V. Section VI presents the attack tolerant data forwarding and summarizes the adaptive and channel-aware forwarding evaluation scheme. Section VII validates the performance of the proposed scheme by extensive simulation results. Finally, Section VIII concludes the paper and outlines our future works.

## II. RELATEDWORK

Increasing attention has been paid to developing countermeasures against selective forwarding attacks, due to their negative impacts on network performance and information integrity. The basic idea of existing works is to monitor the forwarding behaviors of sensor nodes, which can provide evidence and guidance for attack detection and defense [11].The following existing work literature review is divided into two categories: Acknowledgment based and neighbor surveillance based schemes, according to different monitoring techniques for data forwarding.

Acknowledgment based Defense acknowledgments from different nodes in the routing path to determine the packet loss rate of each hop and detect the attackers[12],[13]propose a scheme that randomly chooses a number of intermediate nodes along a forwarding path as checkpoints to return acknowledgments for each received packet. If suspicious behavior is detected, it generates an alarm packet and delivers it to the source node. [14] Design and Implement an intrusion-detection system, named Enhanced Adaptive Acknowledgments (EAACK), for mobile ad hoc networks. Due to the high load of hop-by-hop acknowledgments,(EAAC) combines a two-hop acknowledgment scheme and an end-to-end acknowledgment scheme to detect the malicious Behaviors and reduce the network overhead. In addition, EAACK adopts a digital signature with acknowledgment to ensure authentication, integrity, and non-repudiation. As an elastic evaluation scheme, the reputation system is also applied to attack detection. Zhang et al. [4] develop an audit-based misbehavior detection system to integrate reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavior audits in ad hoc networks. In [15], the correlations between link errors and malicious drops are investigated to detect selective forwarding attacks. In order to guarantee truthful calculation for the correlations, it is proposed that homomorphism linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of acknowledgments reported by nodes. Neighbor-surveillance based Defense Techniques with the Watchdog hardware [16], sensor nodes can monitor the forwarding behaviors of their neighboring nodes and record The actual packet loss accurately. [5] Investigates a functional reputation based reliable data aggregation method against selective forwarding attacks in clustered WSNs. Each node maintains a reputation table to evaluate the behaviors of its neighbor nodes, based on the forwarding monitoring of the neighboring nodes. The nodes with low reputation values are isolated from the routing path. However the reputation Evaluation is only based on the monitored packet loss during the forwarding. [6] style a continual game based mostly approach to research the collision on selective forwarding attacks in multi-hop wireless networks. In [17], it is proposed that a facet Channel watching (SCM) theme to sight selective forwarding attacks in wireless circumstantial networks. the nodes adjacent to an information

ISSN No: - 2456- 2165

communication route, to represent a facet channel for watching the forwarding behaviors of the nodes on the way. Once misbehaviors are detected, the watching nodes send alarm packets to the supply node through each channels. Besides these 2classes of countermeasures, multi-path routing is additionally a wide applied technique to attenuate the impact of selective forwarding attacks on information delivery instead of sight them [18]–[20]. The concept is to divide every information packet into M shares by a (T, M)-threshold secret sharing rule. every packet share is allotted a TTL (time to live) field and forwarded by a indiscriminately elite neighboring node. because the TTL decreases once every transmission, the random forwarding is continual till TTL decreases to zero. As long because the destination receives T shares, the initial message are often with success reconstructed. In such the simplest way, the information integrity are often bonded. Most of the connected works mentioned higher than will effectively mitigate the negative impacts of selective forwarding attacks on data integrity and network performance. However, they need restricted capability to accurately sight the attacks and determine the compromised sensing element nodes. many recent studies contemplate the conventional packet loss into selective forwarding attack detection for wireless mesh networks [21],[22]. However, each of the works use associate calculable traditional packet loss rate to guage the information forwarding behaviors over an extended amount. Such approaches aren't applicable for the WSNs within the unstable radio atmosphere, wherever the high and time-varied packet loss could considerably scale back detection accuracy. Moreover, in their schemes, a node are known as associate aggressor once the amount of lost packets throughout its forwarding exceeds a precise price. The one-time detection also can turn out an oversized false detection chance for the innocent nodes [23]. In the previous work [10], a name system is exploited to sight selective forwarding attacks by taking the conventional packet loss rate into thought. However, it's supporteda hard and fast analysis threshold and easily isolates all the compromised nodes from the information forwarding methods. In this, it is tend to verify associate adaptive threshold to guage the information forwarding behaviors, which might optimize the detection accuracy of the name system. Moreover, it tends to develop associate attack-tolerant routing theme collaborating with the name system to stimulate the cooperation of compromised nodes for associate improved information delivery magnitude relation.

## III. SYSTEM MODEL AND STYLEGOALS

*A. Network Model:*

It is tend to contemplate a WSN consisting of a group of indiscriminately distributed sensing element nodes, denoted by N, associated a sink node to observe an open space. Every sensing element node sporadically senses the attention-grabbing data from the environment and transmits the detected information to the sink via multi-hop routing among sensing element nodes. Sensing element nodes communicate with their neighboring nodes supported the IEEE 802.11 DCF. The monitored space has associate unstable radio atmosphere, creating the packet loss rates throughout the communications of sensing element nodes considerably accrued and vary from time to time [21].Since sensing element nodes ar deployed within the open space and lacked equate physical protection, they'll be compromised by adversaries through physical capture or computer code vulnerabilities to misconduct in information forwarding. It tends to use PM to denote the compromising chance of sensing element node, that is outlined because the chance that a sensing element node is compromised by the soul. Meanwhile, it tends to assume that sensing element nodes will monitor the information forwarding traffic of their neighboring nodes neighbor watching with Watchdog [16] or acknowledgment based mostly approaches [12]. It implies that a sensing element node will get that what percentage information packets ar forwarded by its forwarding sensing element nodes. Existing works [5], [13] offer a comprehensive study on watching forwarding traffic of sensing element nodes, that isn't the main target of this paper. Since the unstable radio atmosphere causes fluctuated packet loss rates between the neighboring nodes, it's difficult to differentiate the monitored forwarding behavior is traditional or not. for simple understanding of the work, Table I summarizes the oftentimes used mathematical notations.

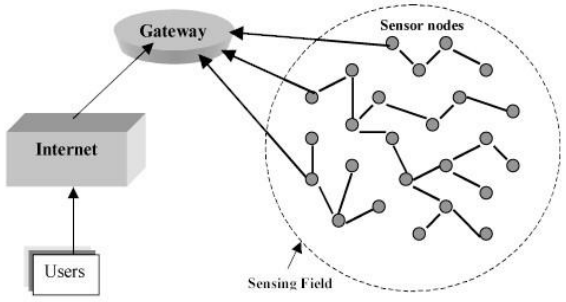


Fig: 3.1 Network model

*B. Attack Model*

Compromised sensor nodes can launch selective forwarding attacks to degrade the performance of the network. Specifically, when a compromised sensor node receives a data packet, it maliciously drops it with a probability, referred to as attack Probability. Since the adversary can control the attack probabilities of compromised nodes, it is difficult to distinguish if the packet losses are caused by fluctuated channel condition or malicious drops, especially for the nodes with low attack probabilities [24].

Furthermore, several neighboring compromised sensor nodes can collaborate with each other to launch promotion/ demotion attacks to achieve benefits [25]. For example, if Na and $N_b$ are two neighboring compromised sensor nodes and data traffic is from Na to $N_b$, Na may provide a partial

ISSN No: - 2456- 2165

evaluation for Nb's forwarding behaviors. Besides, Na can announce $N_b$ as a normal node to its other neighboring nodes, in spite of $N_b$ misbehaving in the data forwarding. However, we do not consider the special case where Na is totally honest in data forwarding to cover for Nb's misbehaviors to achieve benefits. This case can be effectively addressed by the hop-by-hop acknowledgment or two directional neighbor monitoring techniques [4], [22].We consider that cryptographic techniques have been utilized in the network to provide sufficient data confidentiality and authentication against the adversary, then we can focus on resisting selective forwarding attacks. In addition, we assume there are only a fraction of sensor nodes compromised by the adversary to misbehave in data forwarding since the network would be useless if the majority of sensor nodes are manipulated by the adversary. In the following, we call the compromised sensor nodes as malicious nodes and the other sensor nodes as normal nodes.

## IV. CRS-A: THE CHANNEL-AWARE REPUTATION SYSTEM WITH ADAPTIVE DETECTION THRESHOLD

In this section, it is proposed that CRS-A to detect selective forwarding attacks and identify malicious nodes. In CRS-A , every sensing element node maintains a name table to guage the long forwarding behaviors of its neighboring nodes. The essence of CRS-A is to dynamically update the name table supported the forwarding behavior analysis for the neighboring nodes, by taking the conventional packet loss rate into thought. However, because the unstable radio atmosphere create the standard of wireless channel vary with time, traditional packet loss could also be completely different over an extended period. Therefore, we tend to divide the full network life into a sequence of analysis periods T.

In every analysis period Tt, the channel condition of every information transmission link is assumed to be stable. Meanwhile, for every Tt, we tend to introduce a channel estimation stage at the start of Tt, and a name update stage at the top of Tt. throughout the channel estimation stage, sensing element nodes estimate the conventional packet loss rates of the communication links with their neighboring nodes and use them to guage the forwarding behaviors of neighboring nodes. Fig. one shows the summary of analysis periods over the network life. The name updates in CRS-A consists of 3 procedures: name analysis, propagation, and integration. name analysis is to guage short name scores for the forwarding behaviors of sensing element nodes, supported the deviation of calculable traditional packet loss rate and monitored actual packet loss rate. With name Propagation, the evaluated short name scores are often propagated to the neighboring nodes to realize a a lot of comprehensive analysis. Finally, by name Integration, sensing element nodes integrate the name scores evaluated by themselves and also the propagated name scores from their neighboring nodes to update the name table. Fig. two shows the design of CRS-A. In the following, we tend to describe every procedure of CRS-A thoroughly. Since the wireless channel of the WSN is well wedged by unstable radio atmosphere to cause noticeable packet losses throughout wireless transmission, the conventional packet loss ought to be thought of within the forwarding behavior analysis for sensing element nodes. in step with the network model, normal packet loss is especially caused by the poor and unstable wireless channel and MAC layer collisions. We discuss the normal packet loss estimation from the two aspects as follows.

### *A. Packet Loss Caused by Radio Link Quality*

The poor and unstable radio link quality are the primary reason for the time-varied packet losses. In [21], [22], the link condition is formulated as a two-state Markov model, and the packet loss rate is determined as an average value over a long-term period. However, adopting an average value to represent a time varied value may mislead the evaluation for forwarding behaviors [26], [27]. Furthermore, dynamic environments make the link quality varied in different locations. Therefore, the packet loss estimation should be performed in each evaluation period by each sensor node. In CRS-A, the link quality estimation for each pair of neighboring nodes is based on the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR), under the symmetric channel assumption [27], [28].For each Tt, the packet loss rate caused by poor link quality, denoted by p1i,j(t), can be estimated by RSSI and SNR for the transmission link from Ni to Nj.

### *B. Packet Loss Caused by MAC Layer Collisions*

As data transmission between two neighboring nodes is based on the IEEE 802.11 DCF, MAC layer collisions may increase the normal packet loss rate. Since sensor nodes are static in our network, it means each sensor node has a fixed number of neighboring nodes. Then, we can use the analytical results in [21], [29] to estimate the packet loss caused by medium access collisions without the impact of hidden terminals [26], [27]. Let n be the number of nodes contending for channel access at Nj and pt as the probability that a node transmits data in the time slot. When MAC channel is at steady state, the probabilities for observing an idle, successful, and colliding slot, denoted as pi, ps, and PC, respectively.

### *C. Reputation propagation*

In order to share the monitored forwarding behavior information and hence to improve the attack detection accuracy, Ni propagates the first-hand reputation scores, such as r1i,j(t), to their neighbors during each $T_t$. The received reputation scores from the neighboring nodes are called as second hand reputation scores, which reflect the evaluation of the neighboring nodes on their next hop nodes. However, the reputation propagation causes CRS-A vulnerable to collaborative promotion/demotion attacks, which means neighboring malicious nodes can collaborate with each other to

ISSN No: - 2456- 2165

mutually promote their reputation scores [25]. To mitigate the impact of the potentially partial reputation scores, we determine the second-hand reputation scores as follows.

## V. EXISTING SYSTEM

The basic idea of existing works is to monitor the forwarding behaviors of sensor nodes, which can provide evidence and guidance for attack detection and defense. Mainly there are the two existing techniques are used one is Acknowledgment based Defense Technique and another one is Neighbor-surveillance based Defense Technique. However, both of the works use an estimated normal packet loss rate to evaluate the data forwarding behaviors over a long period. Such approaches are not applicable for the WSNs in the unstable radio environment, where the high and time-varied packet loss may significantly reduce detection accuracy.

- *Disadvantages*

Messages over disjoint increase the pollution attacks packets loss is more. A malicious node can attracts all packets by using forged route reply or hidden attack.

## VI. PROPOSED SYSTEM

To improve detection accuracy and packet delivery ration we propose the technique named as CRS-A. In CRS-A, each sensor node maintains a reputation table to evaluate the long-term forwarding behaviors of its neighboring nodes. The essence of CRS-A is to dynamically update the reputation table based on the forwarding behavior evaluation for the neighboring nodes, by taking the normal packet loss rate into consideration. However, as the unstable radio environment make the quality of wireless channel vary with time, normal packet loss may be different over a long time period. Therefore, we divide the whole network lifetime into a sequence of evaluation periods. Based on estimation each sensor stores the packet loss info and then sensor uses the stored info to evaluate the forwarding behavior of neighbor.

- *Advantages*

Help in preventing or avoiding an attack in its initial stage. Hidden attack is not possible QOS is maintained. It can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message.

## VII. ENHANCEMENT

It is proposed that a Channel-aware Reputation System with adaptive detection threshold to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behaviors of sensor nodes, according to the deviation of the monitored packet loss and the estimated normal loss and it optimizes the detection accuracy.

## VIII. ALGORITHM

1) Initialize the Hello timer
2) If Hello timer expires
   a) Send hello message
3) If node has data
   a) If coop checking not yet over
   b) Get the random neighbor from table
   c) Send the req to the neighbor node
   d) Else
   e) Send the req to destination
4) If packet received
   a) If the packet is hello packet
      i) If sender is not malicious
         (1) If node is unknown node
            (a) Add details in table
         (2) Else
            (a) Update the expire time
      ii) Else
         (1) Ignore the packet
   b) If packet is Req packet
      i) Do basic packet filtering and updating operation
      ii) If current node is destination && sender is neighbor
         (1) Set packet as Freq
         (2) Ignore the packet
      iii) If current node is malicious node
         (1) Send reply
      iv) If node is destination
         (1) Send reply
   c) If packet is reply packet
      i) If current node is destination of reply packet && source is neighbor
         (1) Set packet final node is malicious
         (2) Ignore the packet
      ii) Else
         (1) Do normal filtering and updating operation

*A. Packet estimation approach*

If packet is data type

- *Data transfer to the shortest path.*
- Initialize $Trust = 1.000$ for every nodes in a find path.
- Check per every hop count ($Trust = Rx/(Tx * 100)$)
- Calculated value update to Rtable ( $TrustURtable$)

I. If $Trust < 0.75$ && $< 0.25$

- Update node detail into malicious list

Break link

- Generate RREQ to find new route without hacker
- Once again data transfer in another route

ISSN No: - 2456- 2165

II. Else transfer regular data.

## IX. OUTPUT

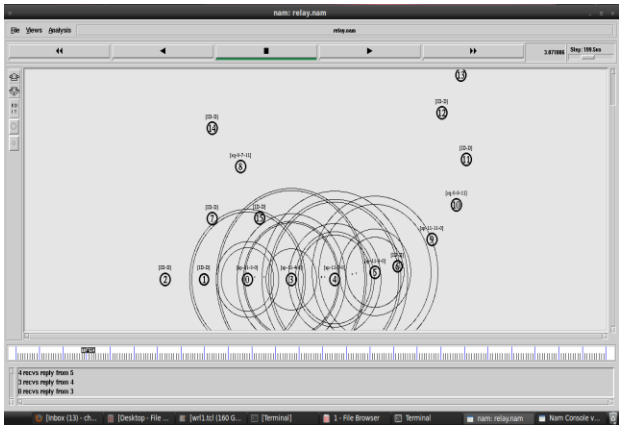

Fig: 9.1.Now SFA attack detect at node 5

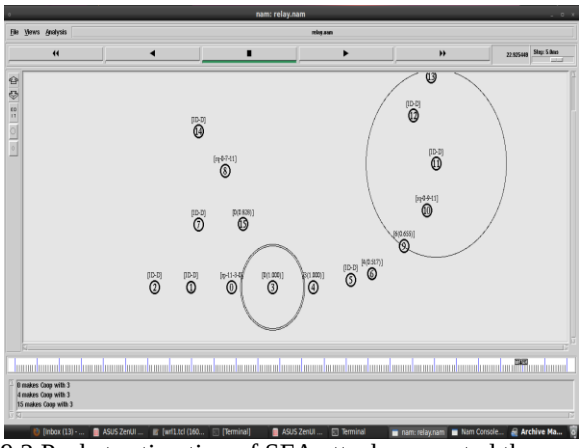

Fig:9.2.Packet estimation of SFA attack prevented the process from node 6 reduce the packet

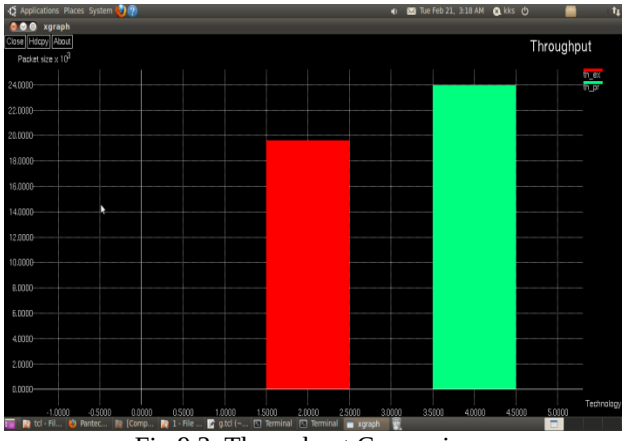


Fig:9.3. Throughput Comparison


Fig 9.4: Delay comparison

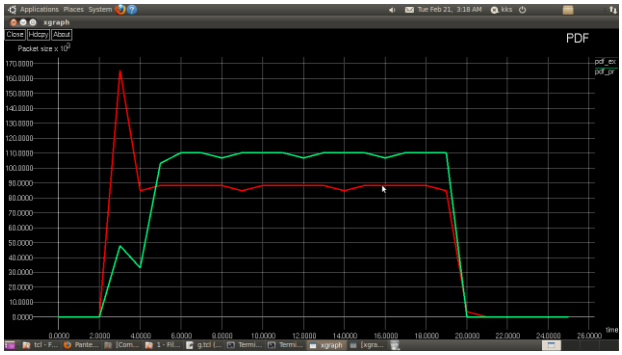


Fig 9.5: Pdf comparison

## REFERENCES

[1] I. Butun, S. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surv. & Tutor., vol. 16, no. 1, pp. 266–282, 2014.

[2] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, 2013.

[3] B. Xiao, B. Yu, and C. Gao, “Chemas: Identify suspect nodes in selective forwarding attacks,” J. Parallel Distributed Comput., vol. 67, no. 11, pp. 1218–1230, 2007.

[4] Y. Zhang, L. Lazos, and W. Kozma, “Amd: Audit-based misbehavior detection in wireless ad hoc networks,” IEEE Trans. Mob. Comput., prePrints, published online in Sept. 2013.

[5] S. Ozdemir, “Functional reputation based reliable data aggregation and transmission for wireless sensor networks,” Comput. Commun., vol. 31, no. 17, pp. 3941–3953, 2008.

[6] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, “A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks,” Comput. Commun., vol. 35, no. 17, pp. 2125–2137, 2012.

[7] X. Liang, X. Lin, and X. Shen, “Enabling trustworthy service evaluation in service-oriented mobile social networks,” IEEE Trans. Parallel Distr. Sys., vol. 25, no. 2, pp. 310–320, 2014.

ISSN No: - 2456- 2165

[8] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Sacrm: Social aware crowdsourcing with reputation management in mobile sensing," Computer Commun., vol. 65, no. 15, pp. 55–65, 2015.

[9] L. Yu, S. Wang, K. Lai, and Y. Nakamori, "Time series forecasting with multiple candidate models: selecting or combining," J. Sys. Sci. Complexity, vol. 18, no. 1, pp. 1–18, 2005.

[10] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in wsns," in Proc. IEEE GLOBECOM, 2014, pp. 330–335.

[11] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges," IEEE Commun. Surv. & Tutor., vol. 13, no. 4, pp. 658–672, 2011.

[12] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," IEEE Trans. Mob. Comput., vol. 6, no. 5, pp. 536–550, 2007.

[13] E. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," IEEE Trans. Vehic. Tech., vol. 60, no. 8, pp. 3947–3962, 2011.

[14] E. Shakshuki, N. Kang, and T. Sheltami, "Eaacka secure intrusion detection system for manets," IEEE Trans. Ind. Electro., vol. 60, no. 3, pp. 1089–1098, 2013.

[15] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in Proc. ACM WiSec, 2012, pp. 87–98.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp. 255–265.

[17] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: packet drop attack detection in wireless ad hoc networks," in Proc. IEEE ICC, 2011, pp. 1–5.

[18] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mob. Comput., vol. 9, no. 7, pp. 941–954, 2010.

[19] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, "Secure and energy efficient disjoint multipath routing for wsns," IEEE Trans. Vehic. Tech., vol. 61, no. 7, pp. 3255–3265, 2012.

[20] S. Li, S. Zhao, X. Wang, K. Zhang, and L. Li, "Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks," IEEE Sys. Journal, vol. 8, no. 3, pp. 858–867, 2014.

[21] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in wmns," IEEE Trans. Wirel. Commun., vol. 9, no. 5, pp. 1661–1675, 2010.

[22] Q. Liu, J. Yin, V. Leung, and Z. Cai, "Fade: Forwarding assessment based detection of collaborative grey hole attacks in wmns," IEEE Trans. Wirel. Commun., vol. 12, no. 10, pp. 5124–5137, 2013.

[23] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions," IEEE Commun. Mag., vol. 53, no. 3, pp. 98–105, 2015.

[24] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," IEEE Commun. Surv. & Tutor., vol. 15, no. 4, pp. 2027–2045, 2013.

[25] H. Lin, X. Zhu, Y. Fang, D. Xing, C. Zhang, and Z. Cao, "Efficient trust based information sharing schemes over distributed collaborative networks," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 279–290, 2013.

[26] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in ieee 802.11-based wireless networks: An analytical approach," IEEE Trans. Mob. Comput., vol. 13, no. 1, pp. 146–158, 2014.

[27] N. Baccour, A. Koubaa, L. Mottola, M. Zuniga, H. Youssef, C. Boan, and M. Alves, "Radio link quality estimation in wireless sensor networks: a survey," ACM Trans. Sens. Netw., vol. 8, no. 4, pp. 1–34, 2012.