ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Intelligent Channel Aware Malicious Free Data Forwarding Scheme Over Wireless Sensor Networks

Shiphrah Sharon Jakkula[1], T. Sunitha[2],

M.Tech. Wireless and Mobile Communications, Department of ETM, G. Narayanamma Institute of Technology And Science (GNITS), Ambedkar Nagar, Shaikpet, Hyderabad, Telangana, India.

Assistant Professor, Department of ETM, G. Narayanamma Institute of Technology And Science (GNITS), Ambedkar Nagar, Shaikpet, Hyderabad, Telangana, India.

ABSTRACT: As a promising event monitoring and data gathering technique, wireless sensor network (WSN) has been widely applied to both military and civilian applications. Many WSNs are deployed in unattended and even hostile environments to perform mission-critical tasks, such as battlefield reconnaissance and homeland security monitoring. However, due to the lack of physical protection, sensor nodes are easily compromised by adversaries, making WSN vulnerable to various security threats. One of the most severe threats is selective forwarding attack, where the compromised nodes can maliciously drop a subset of forwarding packets to deteriorate the data delivery ratio of the network. It also has significantly negative impacts to data integrity, especially for data-sensitive applications, e.g., health-care and industry monitoring. On the other hand, since WSNs are generally deployed in open areas (e.g., primeval forest), the unstable wireless channel requires more concentration and added security with the help of powerful cryptography algorithms, so that a new algorithm is introduced over here with enhanced security norms, called DSA, which takes care of data security with relevant features.

KEYWORDS: CRSA, Channel Aware Reputation System, Wireless Sensor Network, WSN, Data Security, System Threats, DSA, Digital Signature Algorithm.

I. INTRODUCTION

Wireless Sensor Networks (WSN) is a fast growing network scheme and it provides lots of features to communication strategies and routing protocols. Theses routing protocols are introduced to avoid the attacker nodes and provides the efficient communication between source and destination. In this system, a new routing protocol strategy is defined by means of Route Request and Route Response Strategies with the help of Channel Aware Reputation Scheme (CRSA). Source Node sends Route Request to the nearby node. The nearby node checks the request and sends the Route Response to Source Node back within a proper interval. The proper and relevant response from the neighbor node indicates it as a proper node as well as the neighbor node sequence Number will get incremented by 1. The node is proper then only the count will be incremented otherwise it consists attack content. This kind of nodes are properly blocked from the present scenario and the source checks for the alternate or other neighbor nodes to proceed for further communications. As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology. Along with this we improve the data security by means of Digital Signature Algorithm (DSA), which encrypts the content of the transmitting data and extracts back the original data into the recipient end safely. Mobile sink generation is the challenging task for wireless sensor networks (WSNs). In this system we propose to design an efficient routing protocol for single mobile sink and multiple mobile sink for data gathering in WSN. In this process, our main intention is to detect selective forwarding attacks based on the monitored forwarding traffic information and improve the data delivery ratio for WSNs. Specifically, the proposed scheme aims to achieve the following two goals.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

(a) Detection Accuracy: High detection accuracy should be achieved for detecting selective forwarding attacks and identifying the malicious nodes, which can be measured by two metrics. The one is the attacks should be accurately detected once the malicious nodes misbehave in data forwarding. The other is normal nodes cannot be falsely detected as malicious nodes due to the fluctuated normal packet losses.

(b) Data Delivery Ratio Improvement: Besides the detection of selective forwarding attacks, the data delivery ratio of the network should be improved by the proposed scheme to mitigate the negative impacts caused by the attacks. Meanwhile, the proposed scheme should be able to partly stimulate the cooperation of malicious nodes in data forwarding.

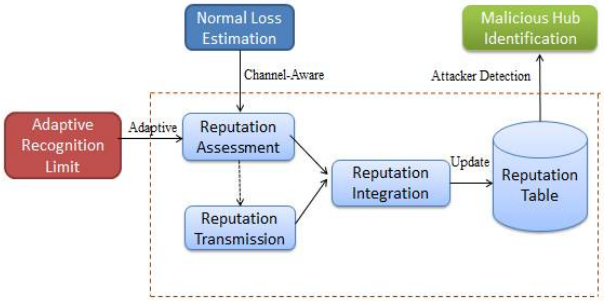

Fig.1. Design of CRS-A

The reputation brings up to date in CRS-A comprises of three methodologies: reputation assessment, transmission and integration. The above fig.1 is the System Design of CRS-A. Reputation Assessment is to assess here and now reputation scores for the sending practices of sensor hubs, in view of the deviation of evaluated ordinary bundle misfortune rate and observed genuine parcel misfortune rate. With Reputation transmission, the assessed here and now reputation scores can be spread inside the neighboring hubs to accomplish a more complete assessment. At last, by, Reputation integration sensor hubs incorporate the reputation scores assessed without anyone else and the transmitted reputation scores from their neighboring hubs to refresh the reputation table.

II. EXISTING RESEARCH SUMMARY

Most of related works focus on monitoring the packet losses in each transmission link and isolating the nodes with high packet loss rates from the data forwarding path. These solutions can improve the data delivery ratio or network throughput but have little effect on detecting selective forwarding attacks. Since the main challenge of attack detection is to distinguish the malicious drop from normal packet loss, the normal packet loss rate of the transmission link should be considered in the forwarding evaluation. The existing work contains several disadvantages, some of them are listed below: (a) More packet losses and high packet loss rate, (b) Higher probability to misbehave in data forwarding and so on.

III. PROPOSED SYSTEM SUMMARY

We propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) 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. To optimize the detection accuracy of CRS-A, we theoretically derive the optimal threshold for forwarding evaluation, which is adaptive to the time varied channel condition and the estimated attack probabilities of compromised nodes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

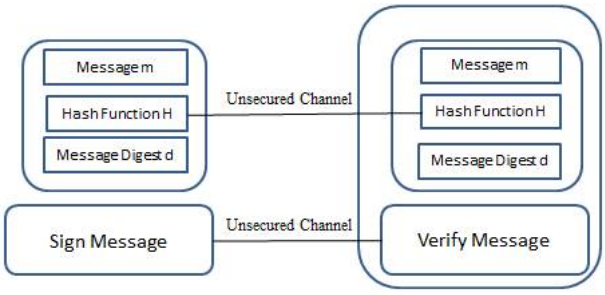

Fig.2. General Flow of Data Using Digital Signature

Furthermore, an attack-tolerant data forwarding scheme is developed to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Extensive simulation results demonstrate that CRS-A can accurately detect selective forwarding attacks and identify the compromised sensor nodes, while the attack-tolerant data forwarding scheme can significantly improve the data delivery ratio of the network. By using Digital Signatures to every parcel to provide sufficient data confidentiality and authentication against the adversary, then we can focus on resisting selective forwarding attacks such that the data is secured from attackers. The proposed work contains several advantages; some of them are listed below: (a) improved data delivery ratio, (b) Improved Accuracy in detection of attacks and so on.

Packet Loss Affected by Radio Connection Quality

The essential explanation behind the time-differed parcel loss in WSNs is because of poor and uncertain radio connection quality. The connection condition is detailed [1], [2] as a two-state Markov show, and the bundle misfortune rate is resolved as a normal incentive over a long haul period. Be that as it may, receiving a normal incentive to speak to time varied esteem may deceive the assessment for sending practices [3], [4]. Besides, dynamic conditions make the connection quality changed in various areas. In this manner, the parcel misfortune estimation ought to be performed in every assessment period by every sensor hub. In CRS-A, the connection quality estimation for each match of neighboring hubs depends on the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR), under the symmetric channel supposition [3], [5]. For every Tt, the parcel misfortune rate caused by poor connection quality, indicated by $P{*}i,j$(t), can be assessed by RSSI and SNR for the transmission interface from Ni to Nj.

Packet Loss Affected by MAC Layer Impacts

As information transmission between two neighboring hubs depends on the IEEE 802.11 DCF, MAC layer impacts may expand the typical parcel misfortune rate. Since sensor hubs are static in our system, it implies every sensor hub has a settled number of neighboring hubs. At that point, we can utilize the explanatory outcomes in earlier systems to assess the parcel misfortune caused by medium access crashes without the effect of concealed terminals. Give n a chance to be the quantity of hubs battling for channel access at Nj and pt as the likelihood that a hub transmits information in scheduled time slot. At the point when MAC channel is at stable state, the probabilities for observing an idle, successful, and colliding slot, symbolized such as Pi, Ps, and Pc, correspondingly, are

$$Pi=(1-Pt)nPs=n.Pt.(1-Pt)n-1Pc=1-Pi-Ps \quad (1)$$

Then the channel busy ratioRb can be evaluated as

$$Cb=1-(Pi.td)/(Pi.\sigma+Ps.ts+Pc.tc) \quad (2)$$

Where td, ts and tc signify the idle slot interval, the period of a successful transmission, and the period of a collision, correspondingly, which can be controlled by past approach. Along these lines, the parcel loss rate affected by MAC layer impacts $P{**}i,j$ is the likelihood that a hub experiences impacts when it transmits, i.e.,

$$P{**}i,j=1-(1-Pt)n-1 \quad (3)$$

Finally the estimated normal parcel loss rate among Ni and Nj in

$$Tt\ Pi,j=P{*}i,j+P{**}i,j-P{*}i,j(t)P{**}i,j \cong P{*}i,j(t)+P{**}i,j \quad (4)$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Reputation Assessment

In CRS-A, sensor hubs screen their neighbors to assess reputation scores for their sending practices during every assessment period. The assessed reputation scores are named as first-hand reputation scores. In particular, in the information transmission phase of Tt, hub Ni ($Ni \in$ N) accounts the quantity of information parcels sent to its next hop hub Nias Si,j(t), and the quantity of information parcels sent by Nj as fi,j(t). Along these lines, the quantity of information parcels lost in the transmission from Ni to Nj is

$$mi,j\,(t) = Si,j(t)\ fi,j(t) \quad (5)$$

In view of the exchange of the past subsection, we can assess the typical parcel loss rate amongst Ni and Nj as pi,j(t). Since every information packet is transmitted to Nj freely, the information transmission from Ni to Nj can be viewed as a succession of autonomous revised trials. That is to say, if Ni sends L information parcels to Nj, the likelihood of k ($0 \le k \le L$) out of L bundles lost amid the transmission, meant by Pi,j (X = k), takes after a binomial appropriation, i.e.,

$$Pi,j(X-k)=(Lk)(pi,j(t))k(1-pi,j(t))L-k \quad (6)$$

The sending conduct assessment is considered for Nj during an assessment period Tt as an examining test. In the event that Nj carries on typically in information sending, mi,j(t) ought to marginally change around the assessed number of ordinary lost information bundles pi,j(t) · Si,j(t). Be that as it may, when mi,j(t) > pi,j(t) · Si,j(t), with the expansion of mi,j(t), the likelihood of Nj acting mischievously in information sending increases. Keeping in mind end goal to assess mi,j(t), we present a recognition limit $\varphi i,j(t)$ and illustrate the reputation assessment function of Ni to Nj as takes after.

$$ri,j(t)=\{+\delta, if\ mi,j(t)\le pi,j(t).Si,j(t)\ -\delta, if\ pi,j(t).Si,j(t)< mi,j(t)\le -\lambda, if\ mi,j(t)>\varphi i,j(t)\ \varphi i,j(t) \quad (7)$$

Where λ is a penalty factor and is a correction factor. We set $\lambda \gg \delta$ and clarify the function as follows.

(a) If mi,j(t)≤ pi,j(t).Si,j(t), the examining test is adequate, which implies the transmission in the midst of Ni and Nj is effective. In this manner, Ni remunerates a positive δ to Nj.

(b) If pi,j(t).Si,j(t)< mi,j(t)≤$\varphi i,j(t)$, we deliberate it as is a typical variance of pi,jm around pi,j, and rate $-\delta$ to Nj nullify the reputation assessment.

Reputation Transmission

Keeping in mind the end goal to share the monitored sending conduct data and subsequently to enhance the assault discovery precision, Ni transmits the first hand reputation scores, for instance,$ri,j*(t)$, to their neighbors amid every Tt. The acquired reputation scores from the neighboring hubs are named as second-hand reputation scores, which mirror the assessment of the neighboring hubs on their next hop hubs. Nevertheless, the reputation transmission origins CRS-A defenseless against collaborative advancement/demote assaults, which implies neighboring malicious hubs can work together with each other to commonly advance their reputation scores [4]. To relieve the effect of the possibly paltry reputation scores, we decide the second-hand reputation scores as below. The second-hand reputation score of Ni to its neighboring hub Nj is calculated as

$$ri,j**(t)=\Sigma Ri,x\Sigma Ri,ss\in NCix\in NCi,g.\ rx,j*(t)+\Sigma Ri,x\Sigma Ri,ss\in NCi.arx,j*(t)x\in NCi,b \quad (8)$$

Where α is a discipline factor to lessen the weight of the data engendered by the possibly deceptive neighbors and α < 1. Since the long haul reputation estimations of mischievous hubs may diminish subsequent to making trouble in various assessment periods, these hubs are grouped into the deceptive neighbor set and the weights of their transmitting data are lessened by the discipline factor α. To decrease the correspondence overhead of reputation transmission, the transmitted reputation scores can be piggybacked to other information parcels, such as, the occasionally replaced neighbor data.

Reputation Integration

After reputation transmission, the first-hand and second-hand here and now reputation scores ought to be incorporated to refresh the reputation table. Mean Ri,j as the long haul reputation estimation of Nj in Ni's reputation table, and Rm and Rs as the upper bound and lower bound of reputation esteem. We compute the coordinated reputation score as $Ri,j*$(t) = $\sigma ri,j*$ (t) + (1-σ) $ri,j**$ (t), and refresh Ri,j as the accompanying condition.

$$Ri,j=\{Rs,\ if\ Ri,j+Ri,j*\le RsRi,j+Ri,j*, if\ Rs,<Ri,j+Ri,j*<RmRm \quad (9)$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

At this time, σ is the weight factor of the first-hand data and > 0.5. *Rm* And *Rs*are framework parameters that can be picked in view of the framework prerequisites. With the end goal that, the capacity prerequisite of the sensor hubs and the correspondence overhead can be diminished.

IV. LITERATURE SURVEY

In the year of 2014, the authors "J. Ren, Y. Zhang, K. Zhang, and X. Shen"[6], proposed a paper titled "Exploiting channel-aware reputation system against selective forwarding attacks in wsns", in that they described such as: Wireless sensor networks (WSNs) are vulnerable to selective forwarding attacks that selectively drop a subset of the forwarding packets to degrade network performances. Due to unstable wireless channels, the packet loss rate between sensor nodes might be high, especially in hostile environments. Therefore, it is difficult to distinguish the malicious drop and normal packet loss. In this paper, we propose a Channel-aware deputation System (CRS) to identify selective forwarding misbehaviors from normal packet losses caused by poor channel quality or medium access collision. Specifically, CRS is based on normal packet loss estimation and neighbor monitoring. Each node maintains a reputation table to evaluate forwarding behaviours of its neighbours. Reputation value is determined by the deviation of the monitored packet loss rate and estimated normal loss rate. The nodes with reputation below a threshold are identified as misbehaving nodes and isolated from data forwarding paths. Furthermore, we develop weighted reputation propagation and integration functions to improve detection efficiency. Through theoretical analysis and extensive simulations, we demonstrate that CRS can accurately detect selective forwarding attacks and significantly improve the network throughput.

In the year of 2011, the authors "S. Djahel, F. Nait-Abdesselam, and Z. Zhang"[7], proposed a paper titled "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges", in that they described such as: mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse. The special network characteristics, such as limited battery power and mobility, make the prevention techniques based on cryptographic primitives ineffective to cope with such attack. Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails, some economic-based approaches can be adopted to alleviate the attack consequences by motivating the nodes cooperation. As a backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them. In this paper, we make a comprehensive survey investigation on the state-of-the-art countermeasures to deal with the packet dropping attack. Furthermore, we examine the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a sophisticated attack.

In the year of 2011, the authors "E. Mahmoud and X. Shen"[8], proposed a paper titled "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in Multihop wireless networks", in that they described such as: Multihop wireless networks, the rational packet droppers may not relay the others' packets because packet relay consumes their resources without benefits, and the irrational packet droppers intentionally drop packets to disrupt the packet transmission process, which may make Multihop communication fail. Cooperation stimulation mechanisms can motivate the rational packet droppers to relay packets, but they cannot identify the irrational packet droppers. In this paper, we develop a novel mechanism that can thwart the rational and irrational packet dropping attacks by adopting stimulation and punishment strategies (TRIPO). TRIPO uses micropayment to stimulate the rational packet droppers to relay the others' packets and enforce fairness and uses reputation system (RS) to identify and evict the irrational packet droppers. We propose a novel monitoring technique to measure the nodes' frequency of dropping packets based on processing the payment receipts instead of using the medium overhearing technique. The receipts can be processed to extract financial information to reward the cooperative nodes that relay packets, as well as contextual information, such as broken links, to build up the RS. Extensive analytical and simulation results demonstrate that TRIPO can secure the payment and precisely identify the irrational packet droppers with almost no false-positive nodes, which can improve the network performance in terms of packet delivery ratio.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

V. EXPERIMENTAL RESULTS

The following figure illustrates the Node formation and precedence of the proposed system.

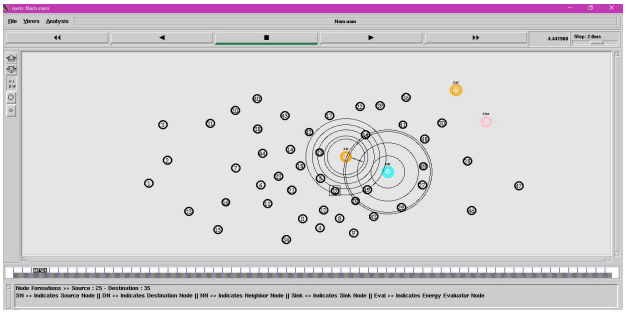

Fig.3. System Precedence

The following figure illustrates the node communication over an environment.

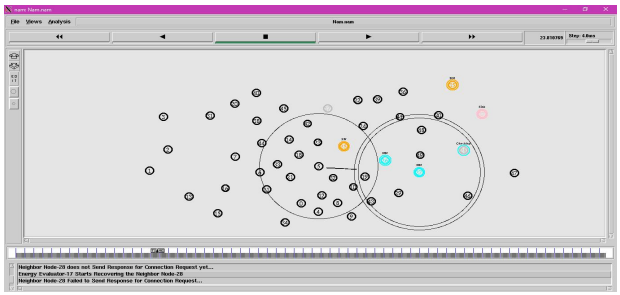

Fig.4. Communication Scenario

The following figure illustrates the Detection Accuracy analysis of the proposed system.

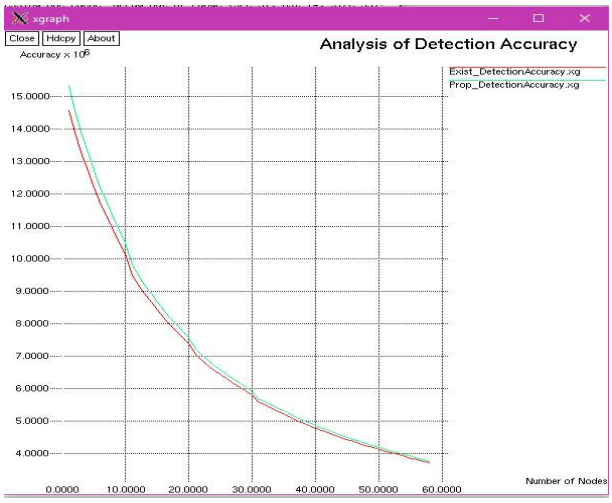

Fig.5. Detection Accuracy Analysis

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

The following figure illustrates the data delivery ratio of the proposed system.

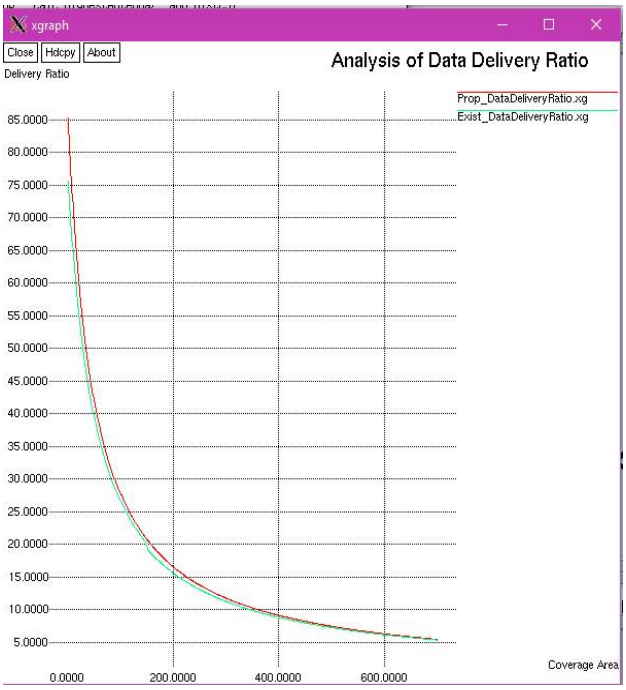

Fig.6. Data Delivery Ratio Analysis

The following figure illustrates the computational time analysis of the proposed system.

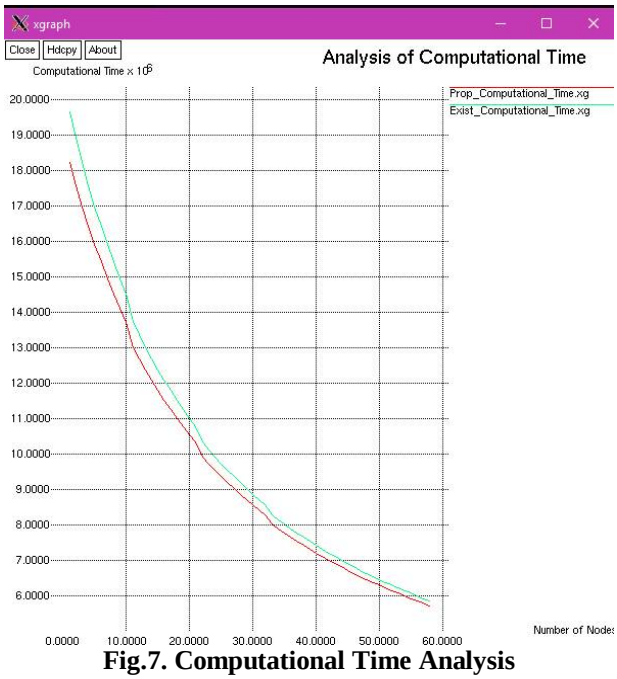

Fig.7. Computational Time Analysis

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

VI. CONCLUSION

In this project, the proposed CRS-A with Digital Signatures to distinguish selective forwarding assaults in WSNs and also to keep data secured from being attacked. To precisely recognize selective forwarding assaults from the typical bundle misfortune, CRSA assesses the sending practices by the deviation between the evaluated ordinary parcel misfortune and monitored parcel misfortune. To enhance the recognition precision of CRS-A, we have additionally determined the ideal assessment limit of CRS-A of every a probabilistic way, which is versatile to the time-changed station condition and the assault probabilities of malicious hubs. On including, a disseminated and assault tolerant information sending design is created to collaborate with CRS-A for invigorating the collaboration of mischievous hubs and upgrading the information delivery proportion. Our Results about demonstrate that the proposed CRS-A with Digital Signatures can accomplish a high recognition precision with low false and missed recognition likelihoods, and the proposed attack tolerant information sending plan can enhance over 12% information delivery proportion for the system and by using the digital signatures the data is secured and the computational time for detecting the malicious hub is reduced.

For future work, we expand our examination concerning WSNs with movable sensor hubs, where the recognition of selective forwarding assaults turns out to be all the more difficult, since the ordinary bundle misfortune rate is more fluctuant and hard to assess because of the mobility of sensor hubs.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] T. Liu and A. E. Cerpa, "Data-driven link quality prediction using link features," ACM Transactions on Sensor Networks (TOSN), vol. 10, no. 2, p. 37, 2014
[6] 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
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] B.Xiao,B.Yu,andC.Gao,"Chemas:Identify suspect nodes in selective forwarding attacks," J. Parallel Distributed Comput., vol. 67, no. 11, pp. 1218–1230, 2007.