WWJMRD 2017; 3(12): 440-446
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Virpal Kaur
Department of CSE,
GZSCCET, Bathinda, India

Abhilasha Jain
Department of CSE,
GZSCCET, Bathinda, India

Correspondence:
Virpal Kaur
Department of CSE,
GZSCCET, Bathinda, India

Detection and Prevention of the Passive Attack in Wireless Sensor Network

Virpal Kaur, Abhilasha Jain

Abstract
WSNs are composed of numerous small sensor nodes which are prone to several active and passive attacks. This paper studies the passive attack in which intruder sends huge amount of packets to the sink node to create congestion over it. Furthermore, trust based scheme to detect and prevent against such kind of attack has been described in the paper. The scheme has been compared against the current approach based on throughput, remaining energy and delay. The scheme has outperformed the prevalent scheme.

Keywords: WSN, passive attack, throughput, delay.

Introduction
The important developments of hardware engineering approaches and effective software processes generate a network of numerous cheap sensors called a wireless sensor network [8-10]. WSN suggests a network for diverse uses for ecological observing and medicinal care. This is extensively used in home safety and battleground investigation situations since WSNs are easy to mount and efficient for such conditions [11]. Nonetheless, in many strategic and unfriendly circumstances, security procedures are mandatory to protect the WSN from the malicious threats [12]. Consequently, security in WSN turns out to be a vital and perplexing task.

There are two key categories of attacks assumed by an intruder. (i) Passive attacks and (ii) Active attacks

Passive Attacks are mentioned to those, which just listen the communiqué. In this type of attack, a stalker watches the communications mutely but does not create any variations in communication. Active attacks are mentioned to those altering communications and creating the wrong data in communication. This paper takes into account passive attack in which intruder sends huge amount of packets to the sink node to create congestion over it. Furthermore, trust based scheme to detect and prevent against such kind of attack has been described in the paper.

Literature Review
In suggested procedure in [1], the authors lessen the passive attack on sink node by reducing the number of messages sent on sink node. The simulation consequences validates that with suggested technique, individual node will compress their information in advance before referring it to cluster head. Subsequently, the message size of node will reduce. This will reduce the message surplus. In this compression method, they decrease the size of message by generating a code sequence of 0 and 1. In this paper [2], the authors are suggesting a technique that can reserve the distinctiveness of the sink node. The simulation consequences validate that the suggested technique can hide the position info of the sink node efficiently and competently. The suggested procedure in [3] can avert numerous types of attacks for example cloning attack, MITM attack and replay attack. The procedure works proficiently and is devoid of producing safety difficulties, since it is zero knowledge based. Each node in the network has exclusive pattern to evade cloning attack. The pattern is reflected as private key. The communiqué happens among nodes until the verifier authorizes the honest nature of

the prover. The system likewise averts passive attacks for instance monitoring and eavesdropping, traffic examination and disguised enemies. The experimental consequences display that the suggested procedure is very active to defend WSN.

In this paper [4], the authors suggest a structure termed General Fake Source (GFS) in contradiction of a universal enemy. It backs the passive RFID, which is without any power source, cannot direct a signal dynamically. Over simulations, the authors demonstrate that GFS soundly unites the performance of actual and false information sources and delivers trade-offs among confidentiality and energy ingestion for source position confidentiality in WSN. This effort [5] presents a new safety structure for wireless sensor networks (WSN) centered on flexible duty cycle, which permits nodes to identify their compromised fellow nodes centered on unexpected variations in network data distribution rate over interval. The structure was measured by its capability to identify progressive WSN dangers (e.g., active, passive, or both attacks). One of the advantages of this structure is that it diminishes all dangers to unexpected power dissipation. In other words, the structure undertakes any neighbor not compatible to projected power levels has been collaborating with an unofficial node, and therefore is not legitimate. This warning prototype is simulated by applying pseudo random but restricted (great to minor) power usages to random nodes. Simulation consequences confirmed that this outline was efficient in identifying and separating negotiated sensor nodes.

This paper [6] examines the influence of two software authenticated encryption with associated data (AEAD) safety concepts on packet throughput of several hop WSN, being counter with cipher block chaining and message authentication code (CCM) and TinyAEAD. Experimentations were carried out in a simulated setting. A case situation is also shown in this study to highlight the influence in an actual domain situation. Consequences detected specify that the safety concepts inspected in this study upset the regular throughput quantities up to three hops.

In this study [7], a novel and safe procedure centered on number theory ideas and congruence calculations has been presented to deliver verification among the sensor nodes and Database Server in a Wireless Network. The suggested procedure practices Fermat Number Transform (FNT) and Chinese Remainder Theorem (CRT) to allow safe communiqué. The procedure will be using its private encryption and decryption process to decrease the computational complication intricate in current procedures. It results in least memory consumption, immediate verification and it survives Cloning attack, Replay attack, DoS attack and Man-in-the-middle attack. Contrast of the current procedure with the suggested procedure is done based on avoidance of numerous attacks and memory competence.

Motivation

The authors in the existing scheme [1] has considered the passive attack in which the attacker node tries to flood the sink node with large number of packets such that sink node remains congested and do not send information further to the users. This will consequently disrupt the purpose of the network. The authors have used the arithmetic compression technique in order to compress the data being received at the sink node. Thus, the load over the sink would decrease. However, it can be argued that compression technique will result in the reduction of throughput at the sink node or over the cluster head in case the attacker is a cluster member. However, the existing scheme suffers from detection technique for such kind of attack. Thus, the proposed scheme tries to give the solution to this.

Proposed Technique

Initially the network will be divided into clusters. The nodes having the highest energy would be preferred as cluster head. Therefore, once the cluster heads are selected, the data transmission will start from the member nodes which aggregate the data at the cluster head.

In first case, the cluster head would monitor at the end of the first round as to amount of data received by each member node. If any node has forwarded data greater than the 20 percent of average amount of data by the cluster members then trust value of the node would be reduced to half of its initial value. If trust value of any node goes to zero, it will be detected as malicious. The cluster head would inform the members to stop communication with it for successive rounds. Secondly, if the cluster head has been compromised then same process will be followed by sink node to detect cluster heads. When the trust value of any CH goes zero, it will mark the node as malicious and inform the other heads and its members to stop communicating with it.

Results

Both the schemes were simulated in NS2.35 and their comparison was done using parameters, namely throughput, remaining energy and delay. Different simulation parameters used in the network were:

Table 5.1: Simulation Parameters

Parameter	Value
Channel	Wireless
Propagation Model	Two Ray Ground
Mac	802.11
Queue	Drop Tail
Antenna	Omni Directional
Number of nodes	50
Number of CHs	6

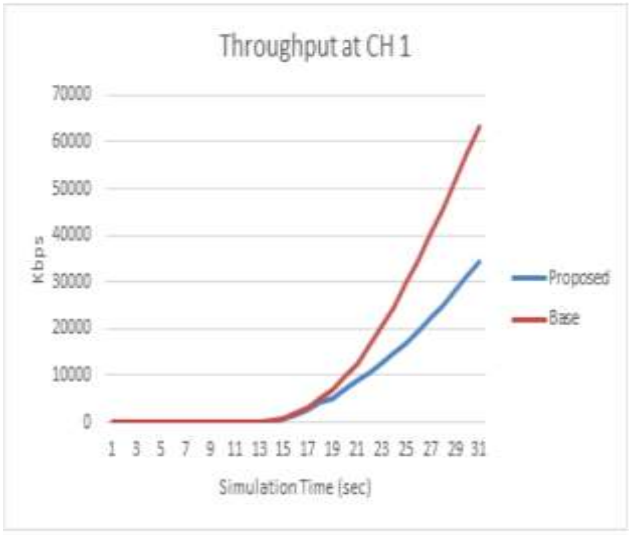

Fig.1: Throughput Comparison at CH 1

This graph shows the value of throughput received at first cluster head per unit of time. The cluster head received approx. 34000 Kbps of data under the proposed scheme as compared to 63000 Kbps under the existing scheme.

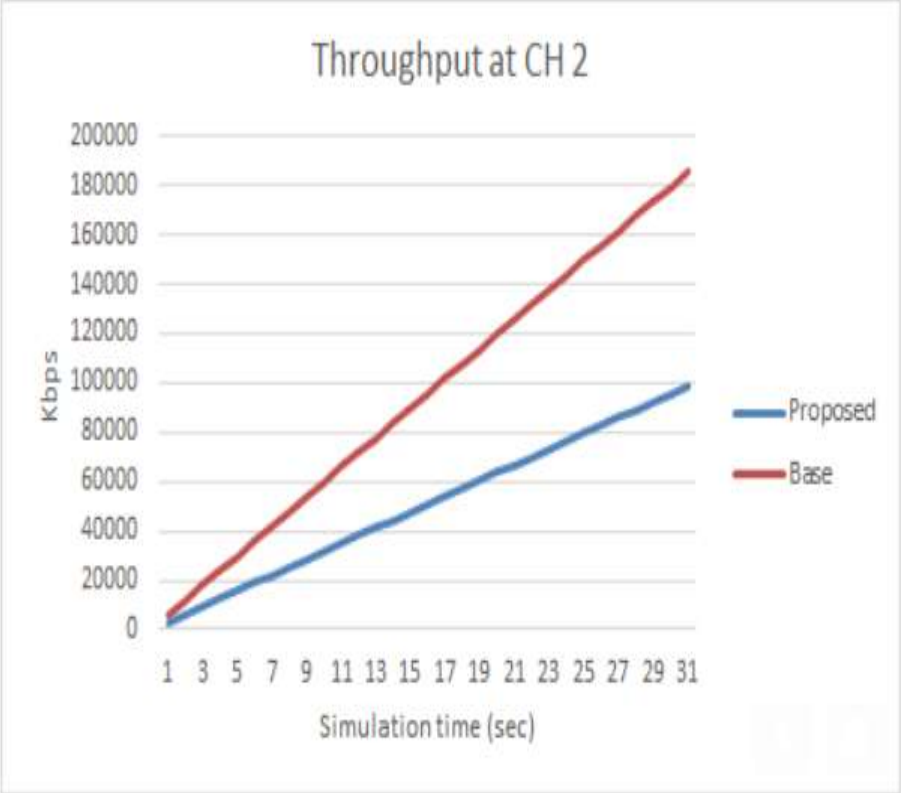

Fig.2: Throughput Comparison at CH 2

This graph shows the value of throughput received at second cluster head per unit of time. The cluster head received approx. 100000 Kbps of data under the proposed scheme as compared to 184000 Kbps under the existing scheme.

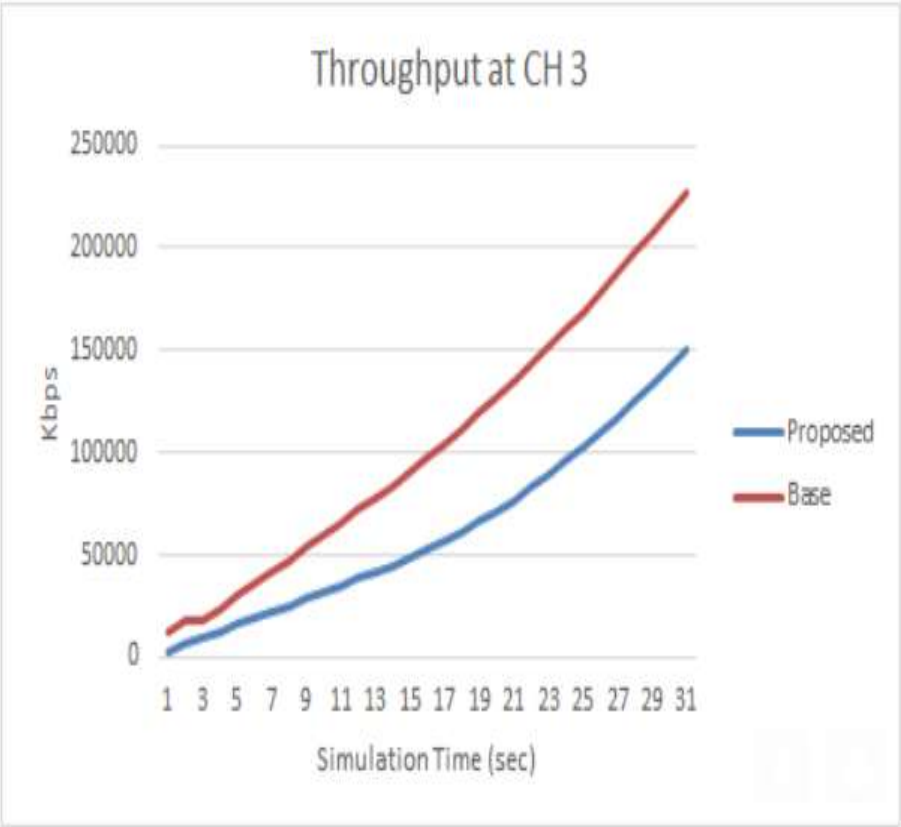

Fig.3: Throughput Comparison at CH 3

This graph shows the value of throughput received at third cluster head per unit of time. The cluster head received approx. 150000 Kbps of data under the proposed scheme as compared to 230000 Kbps under the existing scheme.

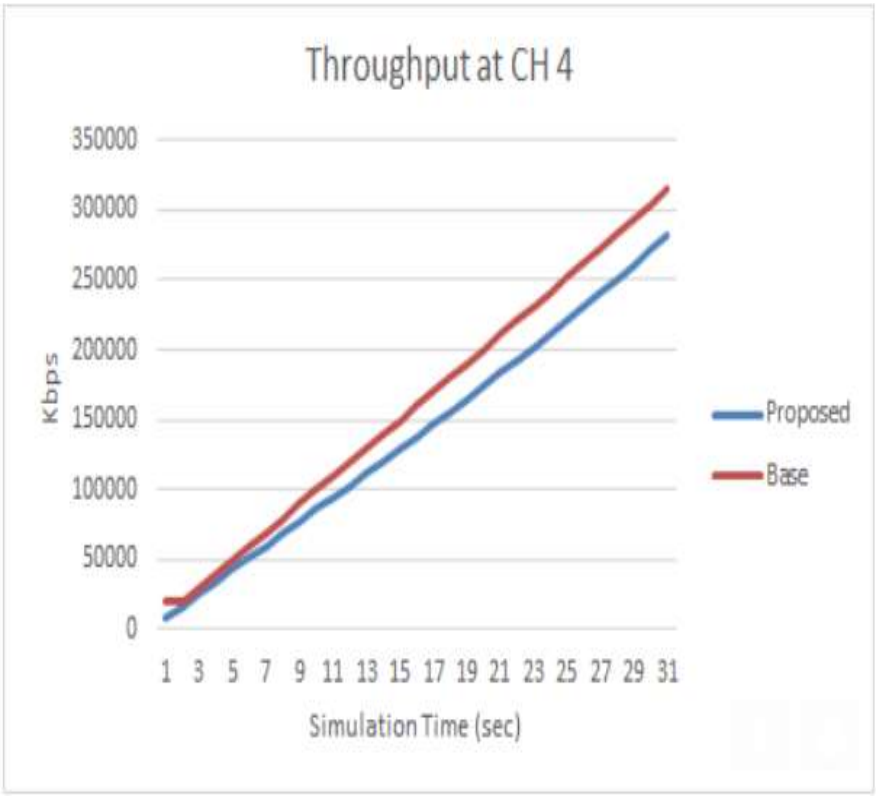

Fig.4: Throughput Comparison at CH 4

This graph shows the value of throughput received at fourth cluster head per unit of time. The cluster head received approx. 270000 Kbps of data under the proposed scheme as compared to 320000 Kbps under the existing scheme.

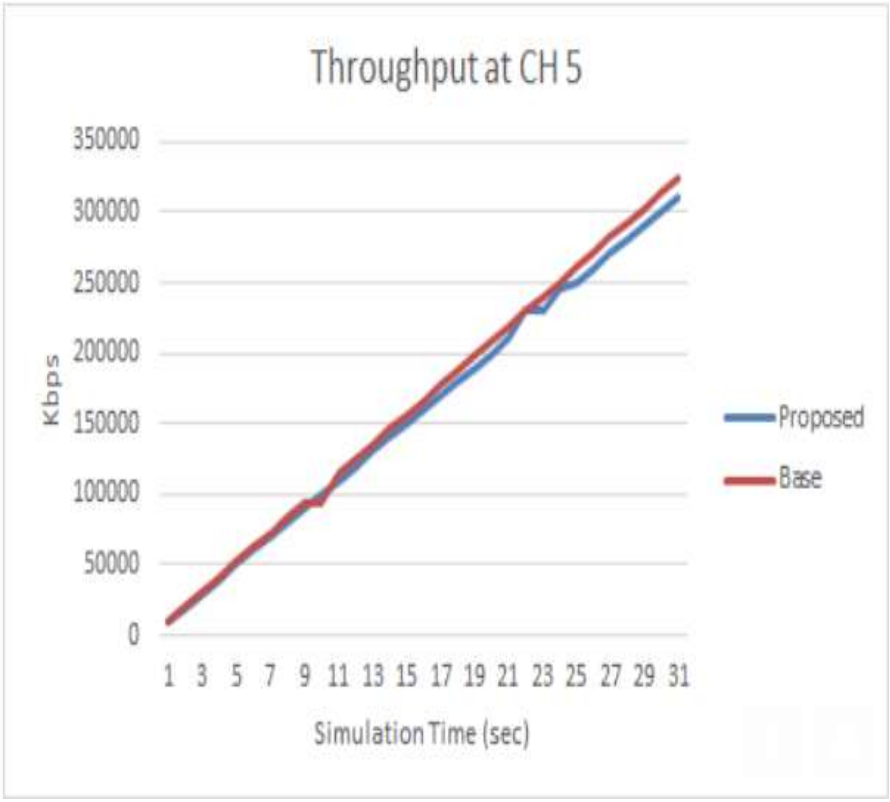

Fig.5: Throughput Comparison at CH 5

This graph shows the value of throughput received at fifth cluster head per unit of time. The cluster head received approx. 310000 Kbps of data under the proposed scheme as compared to 320000 Kbps under the existing scheme.

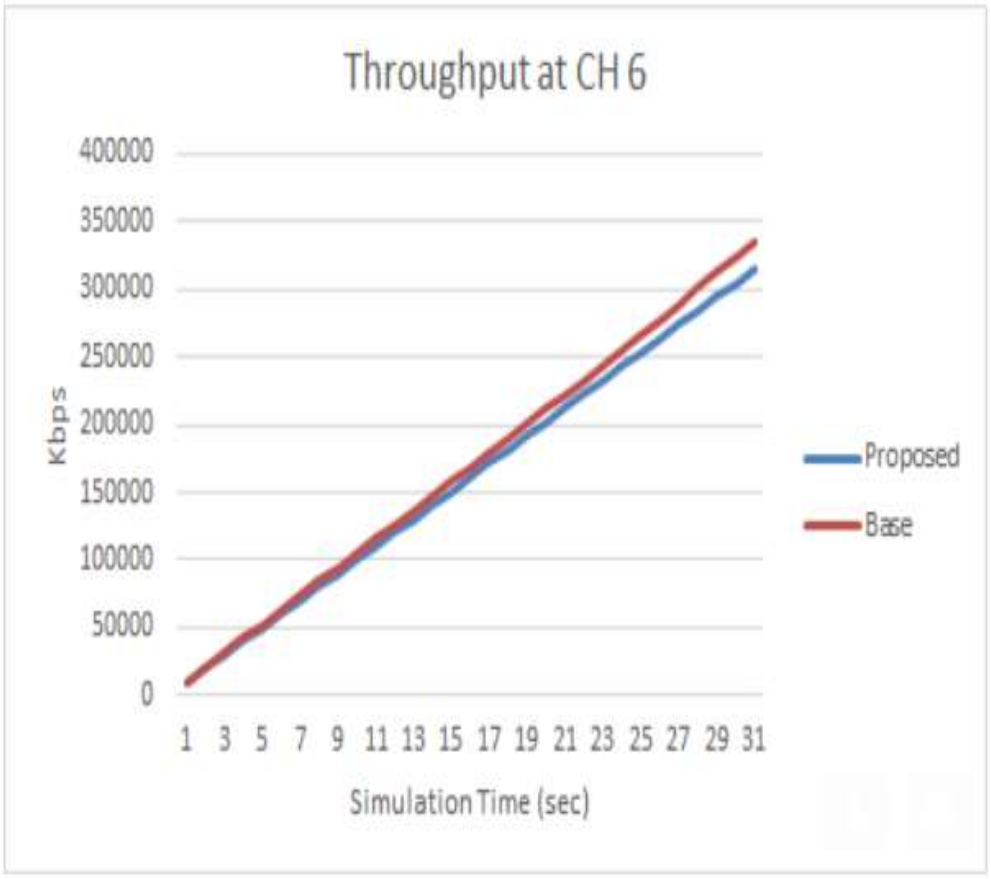

Fig.6: Throughput Comparison at CH 6

This graph shows the value of throughput received at sixth cluster head per unit of time. The cluster head received approx. 320000 Kbps of data under the proposed scheme as compared to 340000 Kbps under the existing scheme.

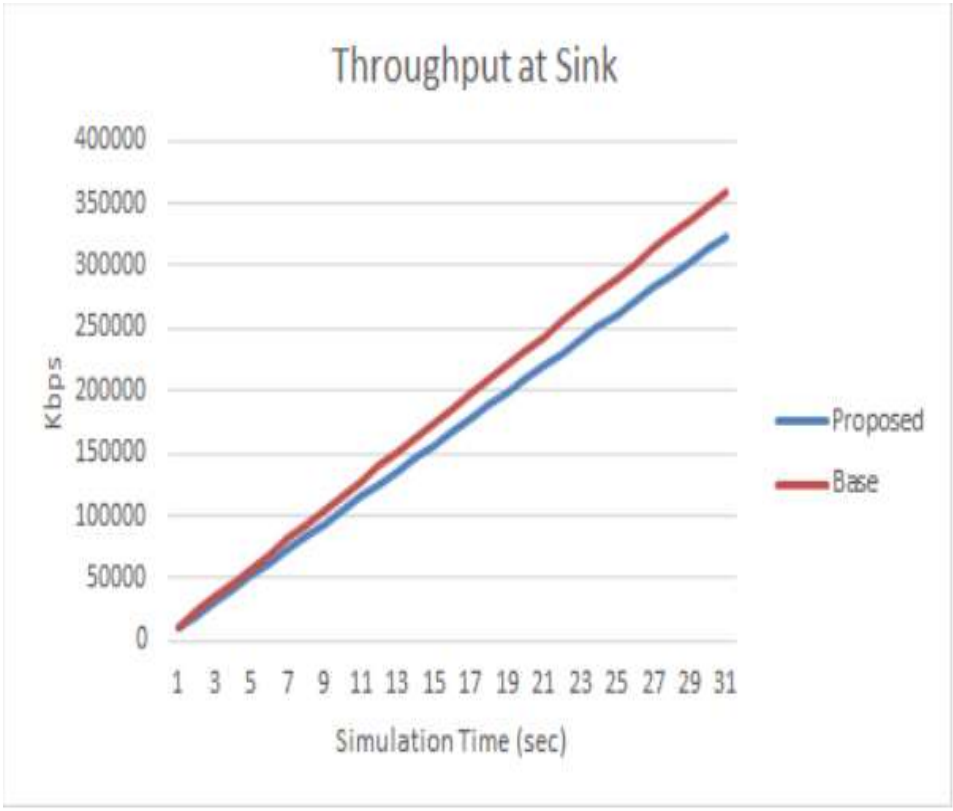

Fig.7: Throughput Comparison at Sink

This graph shows the value of throughput received at sink node per unit of time. The sink received approx. 330000 Kbps of data under the proposed scheme as compared to 355000 Kbps under the existing scheme.

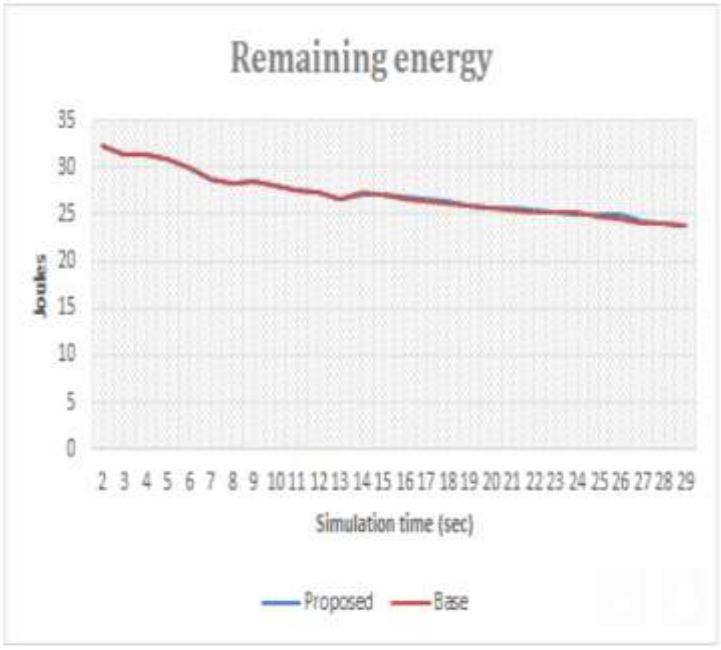

Fig.8: Remaining Energy Comparison

This graph shows the value of remaining energy in the network. Both the schemes consumed almost equal amount of energy in the network but the reduced value of throughput at all the cluster heads as well as the sink shows the successful detection of the passive attacker.

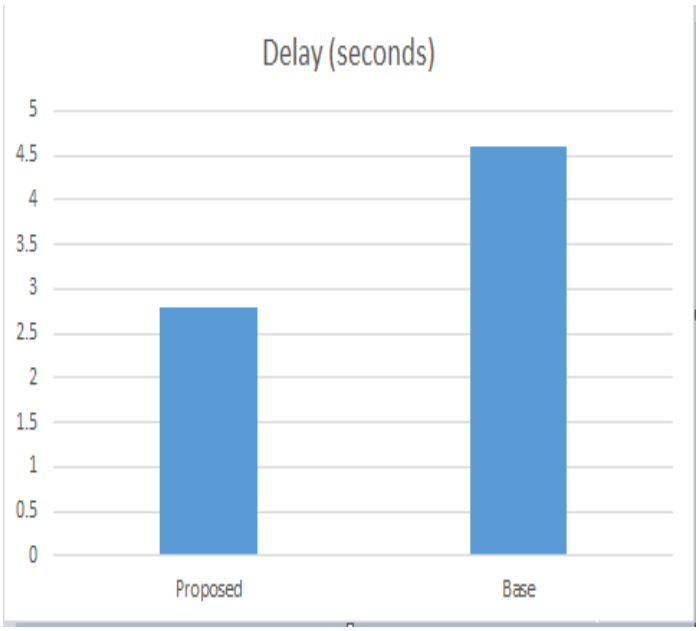

Fig.9: Delay Comparison

This figure shows the comparison of delay generated in the network. The value for delay for the existing scheme was approx. 4.55 seconds and for the proposed scheme it was 2.8 seconds.

Table 5.2: Throughput values received at CH and sink node

Cluster head	Existing scheme	Proposed scheme
1	34000 Kbps	63000 Kbps
2	100000 Kbps	184000 Kbps
3	150000 Kbps	230000 Kbps
4	270000 Kbps	320000Kbps
5	310000 Kbps	320000Kbps
6	320000 Kbps	340000 Kbps
At sink	330000 Kbps	355000 Kbps

Table 5.3: Delay Comparison

Existing scheme		Proposed scheme
4.55 seconds		2.8 seconds

Conclusion

The proposed scheme and the existing scheme were compared based on the throughput at the nodes. The network had six cluster heads and one sink, all these nodes had lesser throughput as compared to the throughput achieved using the existing scheme. Therefore, reduction in the throughput levels shows the successful detection of the malicious node. After blocking communication with the attacker, it cannot take part in the data sending process. This leads to reduction in the throughput levels. This it can

be concluded that proposed is better than the existing scheme. In future, work can be done to secure the network against hello flood attacks, black hole attacks etc.

References

1. Gagandeep Kaur, Deepali, Rekha Kalra, "Improvement and analysis security of WSN from passive attack", 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), IEEE, 2016.
2. Devesh Pratap Singh, R.H. Goudar, Mohammad Wazid, "Hiding the Sink Location from the Passive Attack in WSN", Procedia Engineering, Volume 64, 2013, Pages 16-25.
3. Santhosh S., Radha R., "A Novel Security Model for Preventing Passive and Active Attacks in WSNs", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.
4. Wuchen Xiao, Hua Zhang, Qiaoyan Wen , Wenmin Li, "Passive RFID-supported source location privacy preservation against global eavesdroppers in WSN", 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT), IEEE, 2013.
5. J. M. Chandramouli, Juan Ramos, Lakshmi Srinivasan, Prahlad Suresh, Prashanth Kannan, Garth Crosby, Lanier Watkins, "Using network traffic to infer compromised neighbors in wireless sensor nodes", 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2017.
6. R.D. Sparrow, A.A. Adekunle, R.J. Berry , R.J. Farnish, "Study of two security constructs on throughput for Wireless Sensor multi-hop Networks", 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2015.
7. Manali D. Shah, Shrenik N. Gala, Narendra M. Shekokar, "Lightweight authentication protocol used in Wireless Sensor Network", International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), IEEE, 2014.
8. F. Akyildiz et al., "A Survey on Sensor Networks," IEEE Communications Mag., vol. 40, no. 8, Aug. 2002, pp. 102–14.
9. J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," Proc. ACM Int'l. Conf. Mobile Computing and Networking (MobiCom'99), Aug. 1999, pp. 217–78.
10. G. J. Pottie and W. J. Kaiser, "Wireless Integrated Network Sensors," Communications ACM, vol. 43, no. 5, May 2000, pp.51–58.
11. Shi, Elaine, and Adrian Perrig. "Designing secure sensor networks." IEEE Wireless Communications 11.6 (2004): 38-43.
12. Zhou, Yun, Yuguang Fang, and Yanchao Zhang. "Securing wireless sensor networks: a survey." IEEE Communications Surveys & Tutorials 10.3 (2008): 6-28.