AiMT Advances in Military Technology
Vol. 9, No. 1, June 2014

False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN

A. Babu Karuppiah[1*] and S. Rajaram[2]

[1] *Velammal College of Engineering & Technology, Madurai, India*
[2] *Thiagarajar College of Engineering, Madurai, India*

The manuscript was received on 12 July 2013 and was accepted after revision for publication on 24 June 2014.

Abstract:

A Wireless Sensor Network (WSN) consists of many sensor nodes with low cost and power capability. The nature of WSN makes it easily prone to security attacks and paves way for attackers to easily eavesdrop the network. One of the deadliest attacks is the packet dropping attack by the intruder where the destruction caused to the network becomes inexplicable. It causes the intruder to lure all the packets and drop which will ultimately disrupt the military functionalities. It becomes essential to detect the attacker in split second before rendering heavy damage to the data and the network. Nodes in a WSN are usually highly energy-constrained and expected to operate for long periods from limited on-board energy reserves and there is a high need for energy-efficient operations. In this paper, a novel algorithm is developed to improve the existing Watchdog monitoring system to detect the false misbehaving node and to eliminate it in short time during surveillance. The existing Watchdog mechanism consumes more energy to compute the Sinkhole node in the network and its trustworthiness also becomes debatable. The simulation results show that exact elimination of the malicious node is done. Moreover, a greater percentage reduction in energy consumption is achieved by the proposed method that makes it more viable for military applications to detect the attacker.

Keywords:

Energy efficient mechanism, Military surveillance, Network life time, Sinkhole, Watchdog, Wireless Sensor Networks.

1. Introduction

A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a number of sensor nodes deployed in a specified area for monitoring environment

[*] *Corresponding author: Velammal College of Engineering & Technology, Velammal Nagar, Madurai 625 009, India, phone: +91 0452 2465 289, E-mail: babu_karuppiah@yahoo.co.in*

conditions such as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each other using a wireless radio device. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Most sensor network protocols assume a high degree of trust between nodes in order to eliminate the overhead of authentication. This creates the risk of attackers introducing malicious nodes to the network, or manipulating the operation of existing nodes. Consequently, there is the potential for a wide variety of attacks on sensor networks. An intrusion is defined as a set of actions that compromises confidentiality, availability and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system.

The nodes in WSN are deployed in open air and so they are subjected to a variety of security threats and attacks. Trust mechanism has been developed to defend against insider attacks [11, 12, 15]. Denial of Service (DoS) attacks, Sinkhole, HELLO Flood, Sybil attack, Selective forwarding, Acknowledgement spoofing, Altering or replaying or spoofing routing information are some of the attacks that the nodes are subjected to. The attacks [7] are classified into Active attacks and Passive attacks. The deadliest of the attacks is the Sinkhole attack where its goal of the adversary is to lure all the traffic from a particular area. One motivation for mounting a Sinkhole attack is that it makes selective forwarding trivial. By ensuring that all traffic in the targeted area flows through a compromised node, an adversary can selectively suppress or modify packets originating from any node in the area.

The rest of the paper is organized as follows: Section II deals with the Watchdog Monitoring systems. Section III discusses the related research that has gone into attacks and its detection. The proposed work is dealt with in Section IV followed by the simulation results in Section V. Finally, concluding remarks are given in Section VI.

2. Watchdog Monitoring System

Normal Watchdog is a kind of behavior monitoring mechanism which is the base of many trust systems in ad hoc and wireless sensor networks. In general, trust mechanism works in the following three stages 1) node behavior monitoring, 2) trust measurement and 3) insider attack detection. Watchdog [6] is a popular monitoring mechanism for node behavior monitoring. The basic idea of Watchdog is that a node monitors whether its next-hop neighbor forwards the packets it just sent by overhearing. If the packet is not forwarded within a certain period, the neighbor is regarded as misbehaving in this transaction. The overhearing ability [8] [1] is shown in Fig.1. It is achieved by the use of omnidirectional antennas. The advantage of using omnidirectional antennas is that when a node sends a packet, all its neighbors can hear the node sending the packet. The identity of the node can be verified using existing cryptographic techniques.

Such a technique can be used to verify whether or not a link exists between two nodes. In order for a node to verify whether a link exists between two nodes, it must be within the communication range of both the nodes. In this approach, each sensor

node has its own watchdog that monitors and records its one hop neighbors' behaviors such as packet transmission. When a sending node S sends a packet to its neighbor node T, the Watchdog in S verifies whether T forwards the packet toward the Base Station or not by using the sensor's overhearing ability within its transceiver range. When a node sends a packet to its neighbor, it also cached one locally. Then the node listens to its neighbor's communication. If the neighbor does not forward the same packet to its next-hop node within a period, it is regarded as misbehaving. By this way, a node could record the successful and failed forwarding history of its next-hop.

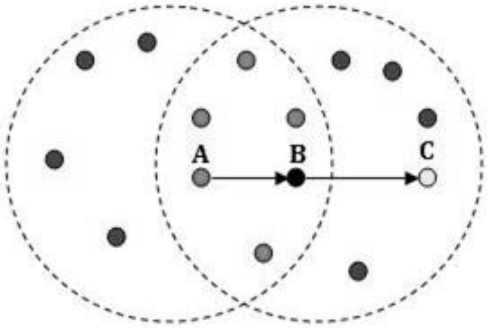

Fig.1 Overhearing ability of nodes in a network

2.1. Limitations of Watchdog Mechanism

Watchdog has some security vulnerabilities due to inherent weaknesses of WSNs such as distributed sensors, limited transceiver range, and multi-hop routing. Watchdog has the limitation [7] of not being able to detect a misbehaving node in the presence of the following cases. The cases are examined using the scenario as shown in Fig. 2 using the path S – A – B – C.

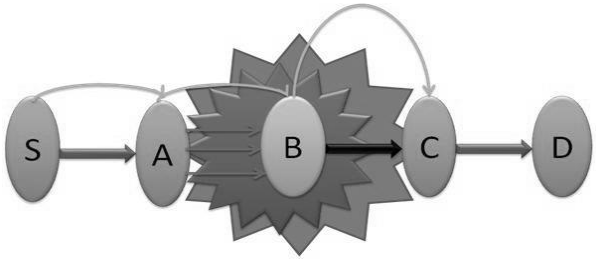

Fig. 2 Limitations of Watchdog Mechanism

1) Ambiguous Collision: Consider the situation that A forwards a packet to B and then starts to overhear whether B will forward the packet to C. However, when B forwards to C, A may not overhear this transmission if other neighbors (such as S) send packets to A at the same time. This ambiguous collision may mislead A to conclude that B is malicious, which may not be correct.

2) Receiver Collision: Similar to the above case, collision may also occur at the receiver side C resulting C does not receive the packet correctly. A can only overhear that B has forwarded the packet, but A cannot tell whether C has received. When this happens, (malicious) node B can intentionally skip retransmissions or (malicious) node

C can generate collision on purpose to avoid receiving the packet and to force B into retransmitting.

3) Limited Transmission Power: If B adjusts its transmission power such that A can overhear but C cannot receive, B can drop packets and increase its trustworthiness (to node A). In geographic routings where every node knows the positions of itself and its neighbors, B can easily launch this attack by selecting a node C from its FS such that dist (B, C) > dist (B, A) where dist (i, j) is a distance between node i and j.

4) False misbehavior: This case happens when a malicious node intentionally reports that other nodes are misbehaving. For example, A may report B is dropping packets although B is not. Then, A's neighbor such as node S, who cannot directly communicate (and thus monitor) B, will consider B malicious.

5) Collusion: Multiple colluding attackers can launch more sophisticated attacks. For example, two malicious colluding node A and B can completely deceive S if A forwards all packets from S to B, but B drops all the packets. Because S cannot overhear B's misbehaviors, S will not consider A and B malicious.

6) Partial dropping: Instead of dropping all packets, B can drop only some packets such that the failure tally will not exceed the detection threshold of A's Watchdog. This is similar with greyhole attack.

3. Related Work

So far, different techniques have been proposed for Watchdog monitoring system in Wireless Sensor Networks. A mechanism based on signal strength [5] was proposed to detect the malicious nodes in a network. The idea was to compare the signal strength of a reception with its expected value. A signal is only detected by a receiving node if the received signal power is equal or greater than the received signal power threshold. If the signal power received is less than the threshold then the particular node is suspected to be malicious. This may not be true for all cases. A signal power can be weakened due to various reasons like environmental factors, weak signal strength etc.

Youngho Cho et al. [13] proposed an improved Watchdog monitoring system by adding a threshold mechanism. In this mechanism, the sending node stores all recently sent packets in its buffer and compares each packet with the overheard packet to see whether there is a match. If yes, it means that the packet is forwarded by the neighboring node and the sender will remove the packet from the buffer. This methodology requires sniffing enough data packets to decide whether a node is an attacker. This means that more time is needed to make a decision compared to a network without a tolerance threshold. If the attacker is moving, there is a possibility that the malicious node moves outside the Watchdog signal range, and thus it could not be detected.

The authors of [14] have used neighbor-based approach in order to mitigate selective forwarding attacks. Wang Xin-sheng et al. in [10] used a monitoring neighbor that alarms the sending node and the Base Station when an insider attacks by dropping packets. The limitation of this method is when neighbor nodes falsely accuse good nodes of attackers. Moreover, it can also not address selective forwarding issue [19].

Bin Xiao et al. [12] used a scheme for detecting selective forwarding attacks. Here, relative communication overhead in terms of number of compromised nodes seems to be higher. In [11], the authors Issa Khalil et al. have proposed an algorithm Unmask for detection, diagnosis and isolation of nodes launching control attacks such

as Wormhole, Sybil, rushing, Sinkhole, and replay attacks. But, the limitation of the methodology lies in its difficulty using for mobile networks.

In [7], the authors have proposed a methodology of monitoring the neighbor by virtually extending the nodes' monitoring coverage. The disadvantage of this method is that the selective packet drops are not addressed. Forootanini et al. [1] have developed an improved Watchdog monitoring system based on a power aware hierarchical model. The methodology resolves the ambiguous Collision.

4. Proposed Work

Existing Watchdog mechanism has the limitation of not being able to detect the misbehaving nodes which upsets the routing of packets in the network. Our objective is to improvise the monitoring of malicious nodes that lead to efficient energy operation and accurate detection of malicious nodes. A novel detection algorithm is devised to detect the fake node that has been pinpointing others to be malicious. The proposed detection Algorithm is as follows:

ALGORITHM 1

Let the WSN has a collection of sensor nodes $N_0 - N_n$.
The source sends data packets to nodes

```
for each intermediate node on a routing path from the Source to Sink
    Sink verifies their sequential numbers
if Sink detects a discontinuous sequential number
    Sink broadcasts an alert packet
end if
for each intermediate node receiving the alert
    it verifies the packets within its cache
  if it detects a missing packet
    sends back an alert to Sink
  else
    sends back a normal response packet
  end if
end for
if Sink receives a collection of response packet
  if an intermediate node does not send back a response
  Sink records the identity of that intermediate node
 end if
 Sink analyzes the status information of the nodes on the routing path
 Sink finds out the malicious nodes
 Sink broadcasts the identity of malicious nodes
end if
end for
```

The sink of the WSN receives the packets that the nodes respond to it in the routing path. It further analyses for the malicious nodes. Let it be assumed that the node responds with a 1 as its status bit for a negative packet and 0 for a positive packet. The node that does not respond has a status bit value to be –1. A suspicious set is generated that contain nodes having status bit as –1. They are not concluded as malicious nodes since the packets from nodes may not have been received by the sink due to

interference and low communication quality. The sink gathers the status bit in subsequent packet transmissions. A suspicious point is set for the node which has the previous status bit as 0 or –1 and if there is a transition to 1 in subsequent data collection. Thus, the sensor node on the routing path where the value changes from 0 or –1 to 1 is referred to as the suspicious point. The node identified as suspicious along with the upstream nodes and downstream nodes form the malicious sequence. Implementation of this concept in the existing Watchdog mechanism enhances the performance by eliminating the misbehaving node accurately without becoming highly time consuming and energy inefficient.

ALGORITHM 2

Let S_0 – Source node ;S_i, S_{i+1}……S_n – Input node ; S_k – Sink node; S_{mi} - Malicious node

1. **for** each S_i watches S_{i+1} whether data sent successfully or not
2. At the same time S_0 sends the data to the S_i
3. **if** S_{i+1} is a true node
4. response bit of S_i is zero
5. **else**
6. response bit of S_i can send zero or one
7. **end if**
8. **end for**
9. When it reaches S_n all the response bit will be sent to the S_k
10. By fixing the suspicious point the exact S_{mi} will be found out.

The property of the malicious node is that it can limit its transmission power and deceive the Watchdog. The proposed algorithm helps to exactly detect such misbehaving nodes. A simple case is taken to analyze the proposed algorithm to find the accuracy of detecting the malicious node and thereby eliminating the false misbehavior limitation of Watchdog mechanism.

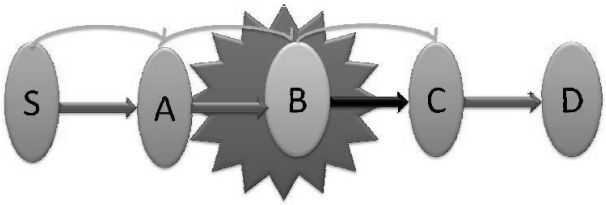

Fig. 3 Scenario of Node B limiting its transmission power

Fig. 3 depicts the scenario of a malicious node limiting its transmission power. The source node is S, the destination being D and the others are the intermediate nodes. In the existing Watchdog mechanism, when B limits its transmission power, it makes the Watchdog to believe that the packet has been sent. Actually, the packet gets dropped without the destination receiving it. As the Watchdog cannot overhear the receiver it assumes that the receiver has receive d the packet and declares the malicious node to be true node and in the process the true node C is falsely declared as malicious when actually node B is. This false misbehavior detection is eliminated in the proposed technique in which the responses from the Watchdog mechanism are considered as the response packets f or the sink node. The packets are sent through the nodes in the

network. A list of status bits is kept for the nodes on the routing path after the sink receives all the response packets from them within a limited time cycle. The status for one round of response can be denoted by a vector $[b_1, b_2, \ldots, b_i]$, $\{1, 0, -1\} \forall$ ib. The sink can perform intrusion detection by analyzing the status vector. To any, b_{i-1}, b_i B, if b_{i-1}=0 or –1 and b_i = 1, then b_{i-1} is a change point in B. A change point is a sensor node on the routing path where the value of status bit turns from 0 or –1 to 1. If a node S_c is a suspicious point and S_{cd} is the nearest downstream node on the routing path, then the sequence (S_c, S_{cd}) contains a malicious node. The major goal of the proposed algorithm is to find those smallest malicious sequences on the routing path. The smallest malicious sequence always contains a suspicious point as well as the nearest downstream node of the suspicious point.

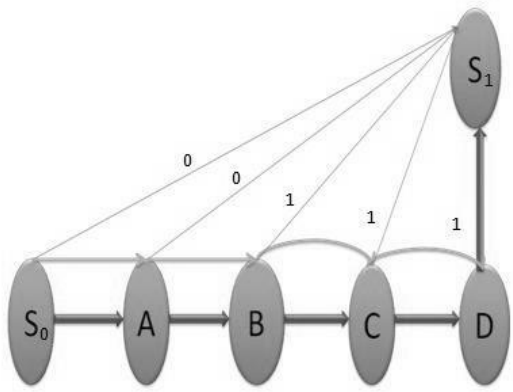

Fig. 4 Implementing the proposed algorithm in Watchdog Mechanism

The smallest malicious sequence can be found by detecting the suspicious point as well as the nearest downstream node, which contains a malicious node. The implementation of the proposed algorithm is shown in Fig. 4. It shows the response bits of one round of the source node S_0 and the intermediate nodes A, B and C being sent to the sink node S_1.

Tab. 1 Response bits of two rounds of the nodes

Node	Round 1	Round 2
S	0	0
A	0	–1
B	1	0
C	1	–1
D	1	1
E	1	0

Tab. 1 shows the response bits of two rounds of the nodes in the network. By implementing the algorithm in the sink, the data collected by it fixes the suspicion point at node B and from the data of the downstream node it concludes exactly that node A is malicious. The limitations found in existence in Watchdog are eliminated

using the proposed scheme. The sink after detecting the exact malicious node broadcasts its identity to the other nodes so that the malicious node is eliminated from the routing path.

5. Experimental Results and Comparisons

It is assumed that the network setup is static, meaning that the location of the sensor nodes does not change. It is also assumed that the sensor nodes have the same transmitting power except the malicious node being able to change its transmission power. The classical radio energy model [1] is considered where the energy consumption of transmitter and the receiver for a bit is 50 nJ.

Fig. 5 shows the simulation of the nodes in WSN using NS2. Here, a 10 node network is simulated and in this the source node is marked in red and the sink node in yellow.

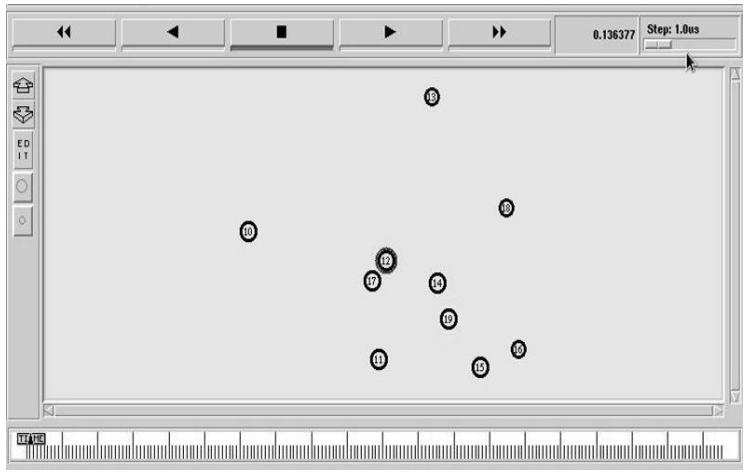

Fig. 5 Scenario of the WSN

Fig. 6 shows the transmission of packets and the response bits to the sink node. The intermediate nodes send the response bits to the sink node. The response bits are collected from the nodes in two rounds to ascertain the exact malicious node.

Once the response bits reach the sink, the algorithm is run in the sink node and a suspicion point is fixed. After careful fixing of the suspicion point node as discussed earlier, the malicious node is accurately determined and the node marked in yellow in Fig. 7 is adjudged malicious.

The identification of malicious nodes in a network is shown in Fig. 8 for both the existing Watchdog mechanism and the proposed algorithm. The graph is plotted for the number of rounds against the nodes. It is found that the existing Watchdog mechanism shows a different node in e ach round to be malicious and to determine the exact malicious node, it takes more rounds and subsequently more energy is consumed in the process. The exact malicious node is identified only twice in the rounds conducted and even then existing mechanism is not unerring as it gives different nodes to be malicious at different times.

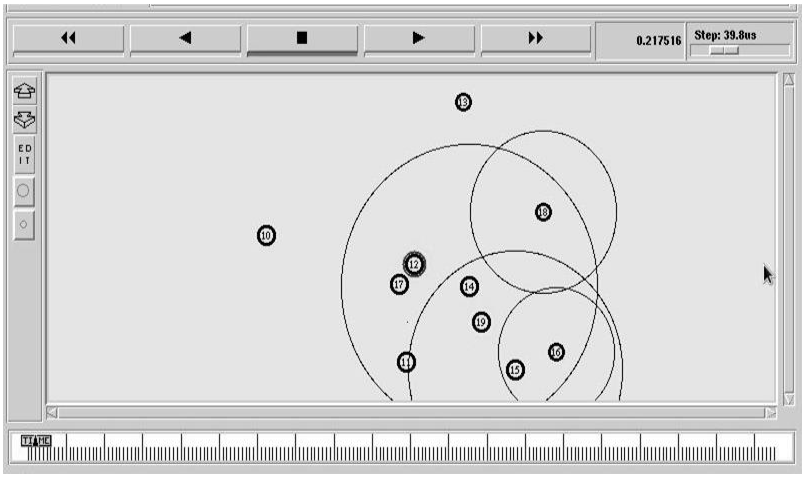

Fig. 6 Transmission of packets and response bits

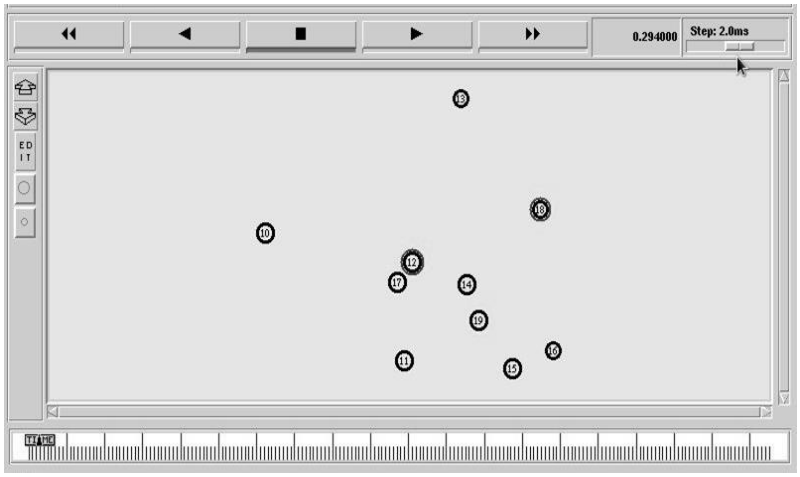

Fig. 7 Detection of malicious node

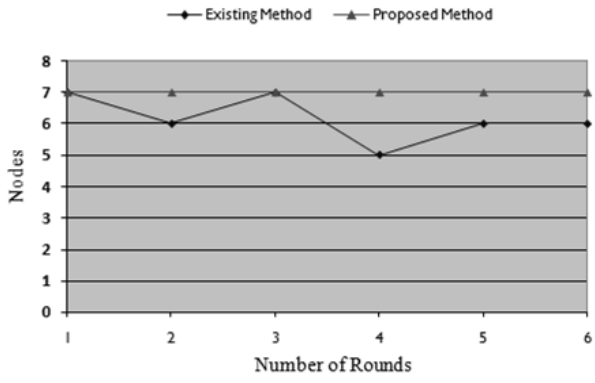

Fig. 8 Identification of exact malicious nodes

The proposed algorithm is found to have identified the exact malicious node irrespective of the number of rounds conducted. All systems, processes and communication protocols for sensors and sensor networks must minimize power consumption. Fig. 9 gives the comparison of energy consumed by the individual nodes in a network. It is seen that the proposed algorithm makes the nodes consume lesser or equal energy when compared with the existing mechanism.

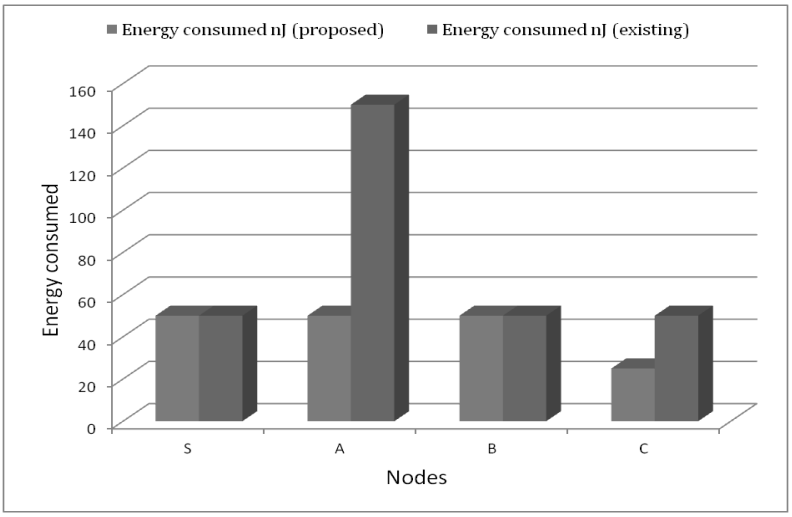

Fig. 9 Energy consumed by individual nodes

The average energy consumption of the network also seems to be low for the proposed algorithm as it is inferred from Fig. 10. The average energy consumed by the network is 43.5nJ when the proposed algorithm is run and it is 75nJ in the existing methodology. This means that nearly 58 % of energy is conserved by the proposed methodology for the network setup taken.

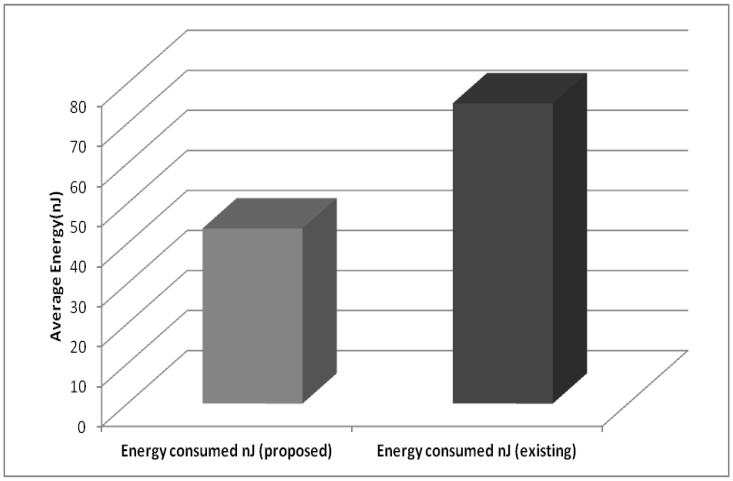

Fig. 10 Average Energy Consumption by the total network

From both the graphs it is inferred that the overall energy consumption and the individual energy consumption are reduced by 58 % using the proposed algorithm when compared with the existing Watchdog methodology.

6. Conclusion

Detection of malicious node in military surveillance is a major concern for security. It is very essential to detect these nodes to prevent the network from loss or tampering of packets. This paper proposes a simple methodology to detect the exact malicious nodes in a Wireless Sensor Network that becomes helpful for military personnel to detect the attacker. By using this methodology the exact malicious nodes can be identified and excluded from the network. The energy consumption of the total network is also considerably reduced. The proposed technique implemented in the sink node eliminates the greatest limitation of the existing Watchdog mechanism, the false misbehavior detection of malicious node. The experimental results also show that the proposed technique consumes lesser energy than the existing method. This reduction in energy by 58% for the network setup taken proves to be very significant for Wireless Sensor Network. This proposed mechanism becomes vital for a dense network consisting of more nodes where only limited power resources are utilized ensuring increase in the life time of the network.

References

[1] FOROOTANINIA, A., GHAZNAVI-GHOUSHCHI, MB. An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS In Wireless Sensor Networks. *International Journal of Network Security & Its Applications*, 2012, vol. 4, no. 4, p. 161-178.

[2] YOUNGHO CHO, GANG QU and YUANMING WU. Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks. In *Proceedings of IEEE CS Security and Privacy Workshops*, IEEE 2012, p. 134-141. ISBN 978-1-4673-2157-0.

[3] TRCEK, D. Trust Management in the Pervasive Computing Era. *IEEE Security & Privacy*, 2011, vol. 9, no. 4, p. 52-55. ISSN 1540-7993.

[4] LOPEZ, J., ROMAN, R, AGUDO, I. and FERNANDEZ- GAGO, C. Trust Management Systems for Wireless Sensor Networks: Best Practices. *Computer Communication*, 2010, vol. 33, no. 9, p. 1086-1093.

[5] VIJAY VARADHARAJAN A Note on Trust-Enhanced Security. *Security & Privacy, IEEE*, 2009, vol. 7, no. 3, p. 57-59. ISSN 1540-7993.

[6] MARTI, S., GIULI, TJ, LAI, K. and BAKER, M. Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*. New York: ACM, 2000, p. 255-265. ISBN 1-58113-197-6.

[7] KARLOF, C. and WAGNER, D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Ad Hoc Networks*, 2003, vol. 1, no. 2-3, p. 293-315.

[8] BAGCHI, S., HARIHARAN, S. and SHROF, N. Secure Neighbor Discovery in Wireless Sensor Networks. *ECE Technical Reports, paper 360*. Purdue University, 2007. Available at:

<http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1362&context=ecetr> [last accessed: 17 May 2014].

[9] TRAN HOANG HAI and EUI-NAM HUH Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge. In *Proceedings of Seventh IEEE International Symposium on Network Computing and Applications*. IEEE, 2008, p. 325-331. ISBN 978-0-7695-3192-2.

[10] WANG XIN-SHENG, ZHAN YONG-ZHAO, XIONG SHU-MING and WANG LIANGMIN. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. In *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. IEEE, 2009, p. 226-232. p. ISBN 978-1-4244-5218-7.

[11] KHALIL, I., BAGCHI, S., CRISTINA N. ROTARU, CN. and SHROFF, NB. UnMask: Utilizing neighbor monitoring for attack mitigation in multihop Wireless Sensor Networks. *Ad Hoc Networks*, 2010, vol. 8, no. 2, p. 148-164.

[12] BIN XIAO, BO YU and CHUANSHAN GAO. CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks. *Journal of Parallel and Distributed Computing*, 2007, vol. 67, no. 11, p. 1218-1230.

[13] LEI HUANG, LIXIANG LIU. Extended Watchdog Mechanism for Wireless Sensor Networks. *Journal of Information and Computing Science*, 2008, vol. 3, no. 1, p. 39-48.

[14] PIRES, WR. Jr., DE PAULA FIGUEIREDO, TH., WONG, HC. and LOURERO, AAF. Malicious Node Detection in Wireless Sensor Networks. In *Proceedings of 18th International Symposium on Parallel and Distributed Processing*. IEEE, 2004.

[15] HAIGUANG CHEN, GANGFENG GU, HUAFENG WU, CHUANSHAN GAO Reputation and Trust Mathematical Approach for Wireless Sensor Networks. *International Journal of Multimedia and Ubiquitous Engineering*, 2007, vol. 2, no. 4, p. 23-32.

[16] WANG, YONG, ATTEBURY, G. and RAMAMURTHY, B. A Survey of Security Issues In Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, 2006, vol. 8, no. 2, p. 2-23.

[17] CALLE TORRES, MG. *Energy Consumption in Wireless Sensor Networks Using GSP* [M.Sc. Thesis]. University of Pittsburgh, 2006, 95 p.

[18] WOOD, AD. and STANKOVIC, JA. Denial of Service in Sensor Networks. *Computer*, 2002, vol. 35, no. 10, p. 54-62.

[19] PATHAN, ASK., ABDUALLAH, WM, KHANAM, S. and SALEEM, HY. *A Pay-and-Stay Model for Tackling Intruders in Hybrid Wireless Mesh Networks. Simulation,* 2013, vol. 89, no. 5, p. 616-633 p.