A Multi Order key Sharing and Dual Channel Based Secure Routing for WSN

Mohammed Abdul Azeem, Khaleel-ur-Rahman khan

Abstract*: Growth in the remote monitoring and automation in maintenance for all fields of industrialization in motivating the sensor researches more and more. The major challenge faced by the practitioners and the researchers are to keep up with the advancements of the data accumulation and analytic demands as the resource capabilities of sensors, especially the wireless sensors, are limited in terms of battery or energy, processing capacity and security. A number of wireless sensor networks collect mission critical and sensitive data for the processing. Also, the feedback systems through the same sensor networks are also important and sensitive. Due to the fragile structure of the network, often it is vulnerable to the attacks. A number of studies have demonstrated the types of the attacks and their effect on the network. The identified attacks are highly versatile in nature, thus leaving a less scope for a single solution to prevent the attacks. Numerous research attempts are presented till date to find the most effective method of securing the wireless sensor networks. Nevertheless, all these solutions are criticised for neglecting one or the other possible threats. It is been observed that, the majority of the attacks happen during the data transmission time and the new node registration time. The transmissions of the data in the network are managed by the routing protocols and the registrations of the new node into the network are managed by node registration algorithms or strategies. Thus, these two are the highly vulnerable situations for any wireless sensor networks life cycle. Hence, this work addresses two unique solutions for these two situations, which is again mutually exclusive. The major outcome of this work is to secure the routing using randomize channels and node registration process using multi order key in order to avoid majority of the attacks on the network. Also, during the transmission or the routing of the data through the network channels, it is often recommended that the data must be encrypted. Nonetheless, the encryption and decryption of the data is a significant load on the limited processing capabilities of the sensor nodes. Thus this highly recommended process is habitually ignored, compromising the threats. Yet another outcome from this work, is to separate the header and the content part of the data packets to reduce the network loads.

***Index Terms*: Secure Routing, Dual Channel, Multi-Order Key, Random Function, Trust Management.**

I. INTRODUCTION

The smarter cities demands a higher number of sensor networks for the industrial, academic and domestic automations. Nonetheless, the wireless sensor based automations can be tedious to maintain due to the flexible structure of the network alongside with the low battery and processing capabilities. The solutions for these smarter cities are limited to specific purposes and cannot cater to all security and performance aspects. The notable works by O. Ozel et al. [1], N. Marlon et al. [2], where the initial process was furnished by G. Ottman et al. [3]. The advancements over the limitations of traditional MANETs as demonstrated by the notable works of A. K. A. Mohammad et al. [4] and G. G. Uttam et al. [5] can be overcome by the use of WSN. The implementations of WSN are not limited to monitoring; rather decisive usages are demonstrated by various research attempts as W. K. K. Chin et al. [6] and Y. Gao et al. [7]. Nevertheless, for a long time, the attacks on the wireless sensor networks were the bottlenecks for implementing higher performing and secure purpose networks. The vulnerability was well furnished by the research attempts of J.G. Choi et al. [8] for fair scheduler, K. B. Sourav et al. [9] by vehicular networks, E. Adel et al. [10] against DoS attacks for all types of services and J.M. Chang et al. [11] for collaborative attacks on nodes. The standard solutions towards these problems as proposed are the encryption methods. Nevertheless, these encryption methods are vulnerable against the recently adopted methods such as multi-hop routings. The rapid energy losses due to the encryption methods are significant and proven by the works of P. G. Fernandoet al. [12], X. Du et al. [13] and J. Lin et al. [14] for secure and private information transmissions. Thus, the trust based mechanisms for handling these risks are getting popular. However, the trust based managements are also not widely accepted due to various reasons. The major reasons are enlisted here: Firstly, the trust based security mechanisms can reduce the chances of inherent security attacks, but can intricate many other types of risks. Secondly, the trust based management schemes can be highly complicated during the incorporations of other performance parameters such as number of hops or the delay or the Quality of the Services.

Finally, the trust based systems demonstrates a high dependency on the route information or the network schema. This can defeat the purpose of using wireless sensor networks.

The limitations stated in this work are well justified by the statements of notable researchers as S. Kurosawa et al. [15], D. Zhu et al. [16], P. Zhao et al. [17] and W. Yu et al. [18]. Thus considering the limitations and the demand of the modern industry, this work proposes a secure routing scheme with the flexibility of dual channel for communication, selected randomly based on secure random function, distribution of the packets by especially designed encryption algorithms and enhanced trust based model for node registrations.

Revised Manuscript Received on 30 September 2018.

***** Correspondence Author

Mohammed Abdul Azeem*, Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad (Telangana), India.

Dr. Khaleel-ur-Rahman Khan, Professor, Department of Computer Science and Engineering, ACE Engineering College, Ghatkesar (Telangana), India.

The rest of the work is organized such that, in the Section – II the parallel research outcomes are elaborated, in Section – III the proposed trust model is furnished, the proposed key sharing method is uncovered in the Section – IV, as this work elaborates on the multi-channel routing process, the details are particularized in Section – V, the complete scheme is explained in the Section – VI, Section – VII explains the results and presents the discussion, the comparative analysis for establishment of the improvements are listed in the Section – VIII and finally the conclusion of this research is presented in the Section – IX.

A. Outcomes from the Parallel Researches

The recent advancements of the parallel research shows good number of attack prevention mechanisms. In this section of the work, elaborates on the attack types and their counter measures. The attacks based on their target types can be classified into two different classes as attacks on routing mechanism and attacks on the trust model attacks. The multi-hop models contribute higher degree of damages to the wireless sensor networks compared to the traditional communication networks. These attacks are mainly on the node aspects by making the node behaviour changes called soft attacks and the attacks directly on the resources [Fig – 1] of the network used for transmission are called the hard attacks.

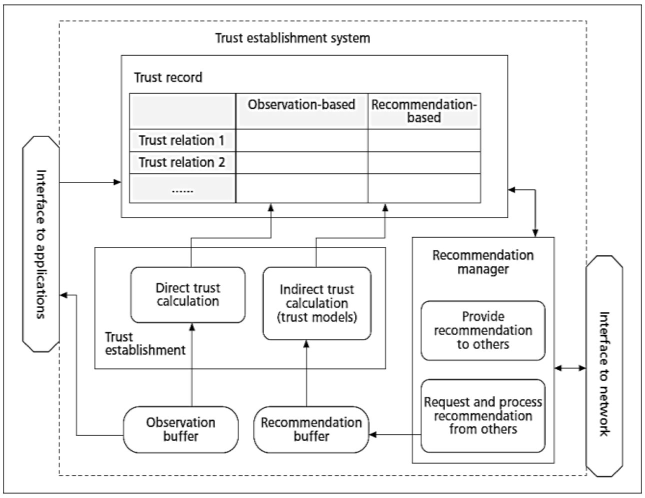


Fig. 1 Trust Based Network Components

The work by R. Morsi et al. [19] demonstrates the effects of malicious node incorporation over fading channels. Also the work of J. Yao et al. [20] demonstrates the effect of grayhole attacks on decode-and-forward relaying networks. The most encountered attacks such as Sybil attacks targeting the identity of the network resources can be highly compromising on the network behaviours as proven by B. Paramasivan et al. [21]. These mentioned attacks can be prevented and recovering from these attacks is less costly. However, attacks which manipulate the network resources and often destroy the network resources are highly costly to recover. In the notable work by I. Krikidis et al. [22] shows the effect of attacks on resource capabilities by exhausting the objects in the network. Also, not only on the physical objects, the attacks repeatedly tamper the bandwidth of the networks as proven by A. Vosoughi et al. [23].

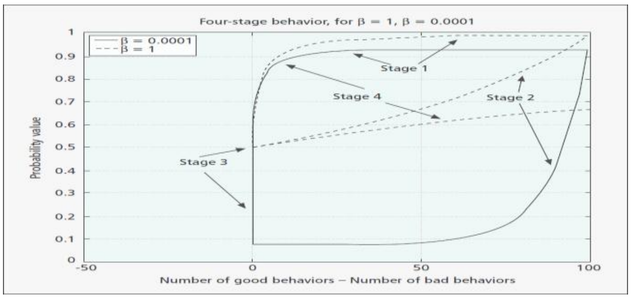


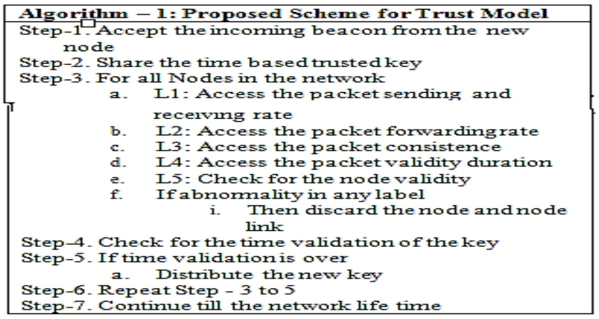
Fig. 2 Trust Based Network System – Attack Phases [25]

As proven by A. Cornejo et al. [24] that most of the attacks can be handled and prevented by the trust based models. Nonetheless, the newer types of attacks can also be intricate by the trust models [Fig – 2]. A number of studies have confirmed that, the attacks such as on off attacks or the conflicting attacks or the selfish attacks or the collusion attacks can be highly possible on the trust based models [25].

B. Proposed Trust Model

The trust based models are generally considered to be deployed in three layers as on the node level, on the cluster head levels, in case of a clustered approach and on the base station level. In this section of the work the novel approach is presented for the proposed trust based model. The novelty of this approach is to consider the parametric factors for establishing the trust based model.

The approach is furnished here:



```
Algorithm – 1: Proposed Scheme for Trust Model
Step-1. Accept the incoming beacon from the new
        node
Step-2. Share the time based trusted key
Step-3. For all Nodes in the network
        a.  L1: Access the packet sending and
            receiving rate
        b.  L2: Access the packet forwarding rate
        c.  L3: Access the packet consistence
        d.  L4: Access the packet validity duration
        e.  L5: Check for the node validity
        f.  If abnormality in any label
            i.  Then discard the node and node
                link
Step-4. Check for the time validation of the key
Step-5. If time validation is over
        a.  Distribute the new key
Step-6. Repeat Step - 3 to 5
Step-7. Continue till the network life time
```

The scheme is visualized graphically as well in [Fig – 3].

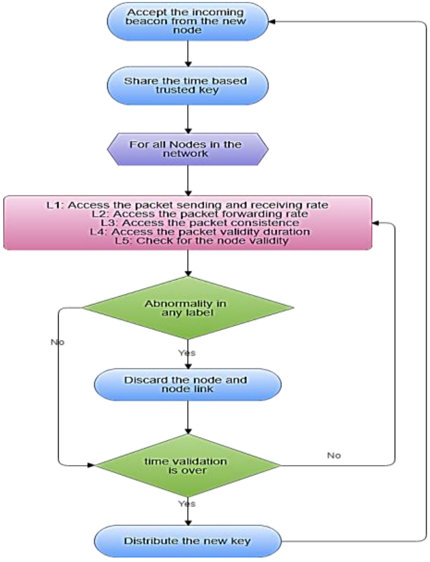

Accept the incoming beacon from the new node
Share the time based trusted key
For all Nodes in the network
L1: Access the packet sending and receiving rate
L2: Access the packet forwarding rate
L3: Access the packet consistence
L4: Access the packet validity duration
L5: Check for the node validity
Abnormality in any label
No
Yes
Discard the node and node link
time validation is over
No
Yes
Distribute the new key

Fig. 3 Proposed Trust Model Scheme

The obtained results from this section is presented and discussed in the further section of this work.

C. Proposed Key Sharing Method

The domain of key sharing depends on the type of keys getting used in the network. As during the installation of symmetric keys, the distribution process is fairly simple and can be fetched from a single location without the hassle. However, in case of the public – private key sharing, the transmission of the keys are to be strategies.

In this work, there are two different keys to be shared as

- The Trust Key: Firstly, as the trust based model proposed by this work, upon validation of the complete process of trust manager, the secure trust key will be distributed to the validated nodes. Further, this trust key is expected to be the deployed during the routing. Regardless to mention this is a symmetric key.
- The Routing Key Set: Secondly, the encryption key for the routing of information is transmitted and with the help of the trust key, the key to decode the header can be achieved. Thus every node must have or generate a total of three keys. Primarily, the trust key, secondly the public key to decode the header and finally the key to encrypt the header for the next node.

The proposed network model is realized in real time and fabricated here in [Fig – 4].

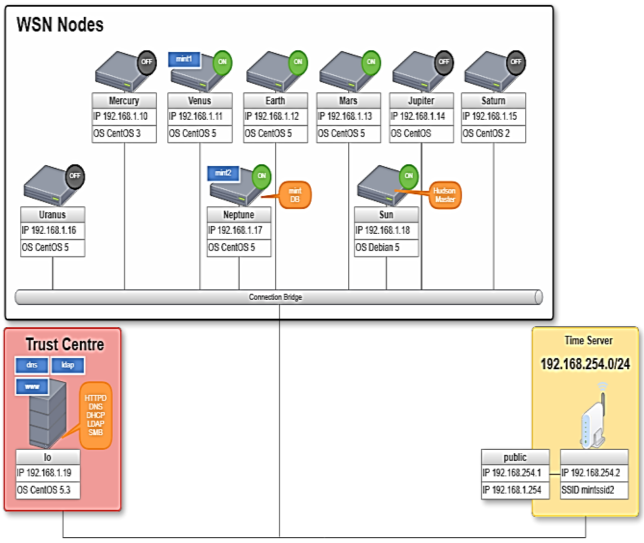
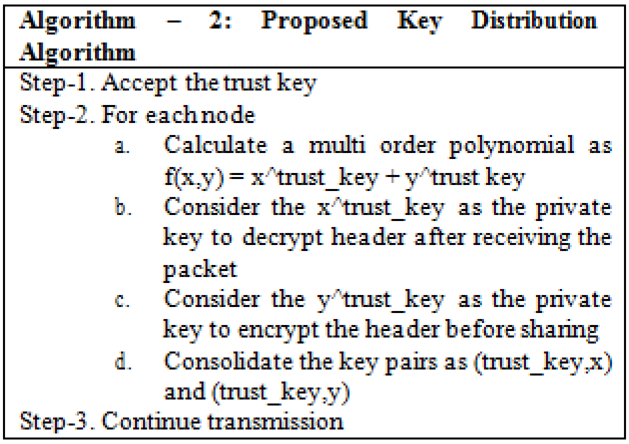


Fig. 4 Key Sharing Network Structure

The proposed algorithm for key sharing is elaborated here:

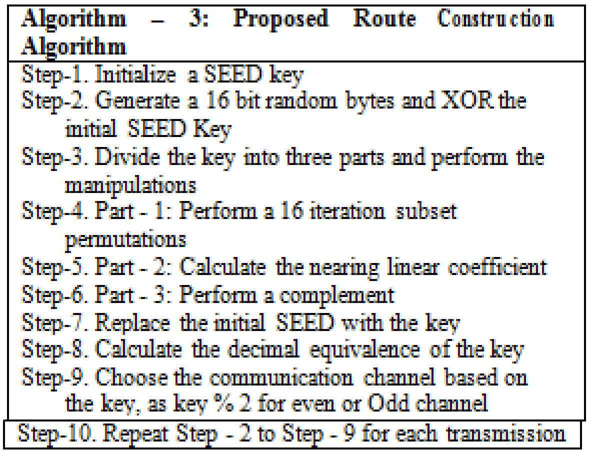


```
Algorithm – 2: Proposed Key Distribution Algorithm
Step-1. Accept the trust key
Step-2. For each node
    a. Calculate a multi order polynomial as $f(x,y) = x^{trust\_key} + y^{trust\ key}$
    b. Consider the x^trust_key as the private key to decrypt header after receiving the packet
    c. Consider the y^trust_key as the private key to encrypt the header before sharing
    d. Consolidate the key pairs as (trust_key,x) and (trust_key,y)
Step-3. Continue transmission
```

It is natural to understand that the random variables x, y are generated using a specific function at the node level and can be adjusted from the trust manager base. The results obtained from this section is presented and discussed in the further section of this work.

D. Proposed Route Construction Algorithm

The major objective of this work is to make the routing protocol more secure, hence this work proposes yet another component in the framework. The primary arrangement of the network is to establish a dual channel of communication between each two nodes. The dual channel for communication works as mutually exclusive. Here, the channels are randomly chosen to transmit the information in order to make the network more stable against the attacks. It is natural to realize that the randomization of the communication channel selection is the key factor. Hence, this work elaborates the route selection process here:



```
Algorithm – 3: Proposed Route Construction Algorithm
Step-1. Initialize a SEED key
Step-2. Generate a 16 bit random bytes and XOR the
    initial SEED Key
Step-3. Divide the key into three parts and perform the
    manipulations
Step-4. Part - 1: Perform a 16 iteration subset
    permutations
Step-5. Part - 2: Calculate the nearing linear coefficient
Step-6. Part - 3: Perform a complement
Step-7. Replace the initial SEED with the key
Step-8. Calculate the decimal equivalence of the key
Step-9. Choose the communication channel based on
    the key, as key % 2 for even or Odd channel
Step-10. Repeat Step - 2 to Step - 9 for each transmission
```

The results obtained from this section is presented and discussed in the further section of this work.

E. Proposed Hybrid Framework

After the detailed elaboration of the individual algorithms, this section of the work formulates the final framework and its component with description.

The hybrid framework is elaborated here [Fig – 5].

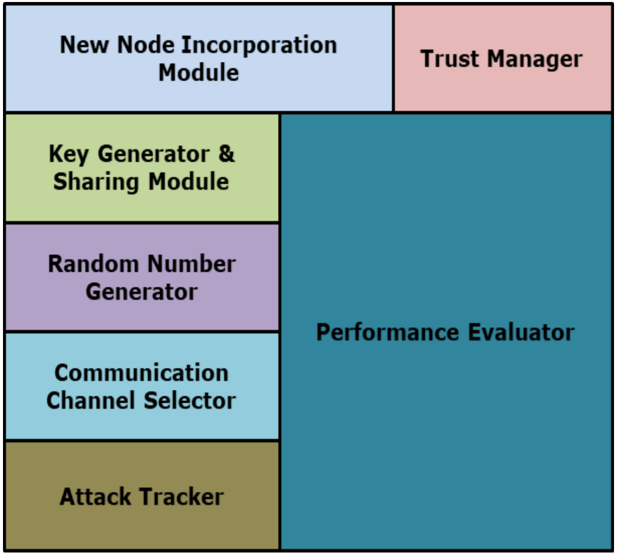

New Node Incorporation Module
Trust Manager
Key Generator & Sharing Module
Random Number Generator
Communication Channel Selector
Attack Tracker
Performance Evaluator

Fig. 5 Proposed Hybrid Framework

F. New Node Incorporation Module

The New Node inclusion or incorporation module in the framework responds to the new node registration signals. This module or component of the framework signals the trust manager to issue the trust based key based on the algorithm and subjected to satisfaction of the parameters.

B. Trust Manager

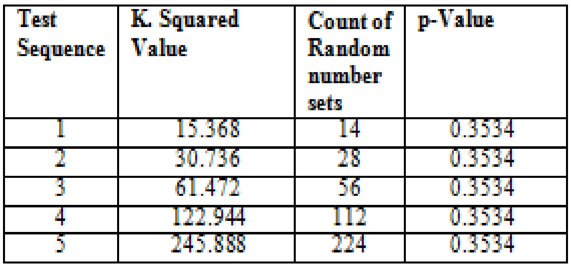
The trust manager component of the framework evaluates the nodes integrity based on the predefined parameter sets such as packet sending and receiving rate, packet consistency, packet forwarding rate, information validity and node validity.

G. Random Number Generator

The random number generator algorithm runs on this component of the framework. The purpose of this component is to generate the random numbers for the route or communication channel selector and the random number generation for encryption algorithms.

The randomness of the numbers generated by this component is also tested and the findings are listed here [Table - I].

Table I: Homogeneity Of Randomness Test



Test Sequence	K Squared Value	Count of Random number sets	p-Value
1	15.368	14	0.3534
2	30.736	28	0.3534
3	61.472	56	0.3534
4	122.944	112	0.3534
5	245.888	224	0.3534

Thus it is natural to understand that, the random number generator algorithm is proven to be highly successful against the Bartlett test.

The distribution of the randomness is illustrated here in [Fig– 6].

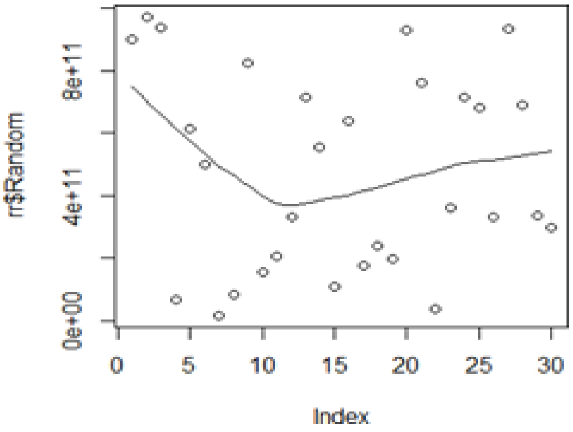


Fig. 6 Randomness of the Distribution

H. Communication Channel Selector

This component of the framework initializes the communication channels for the WSN nodes and accepts the inputs from the Random number generator component. Based on simple principle of modulus operation, the communication channels are selected. If the modulus result of the random number is 0, then the first channel is selected and if the result is 1, then the second channel is selected.

The communication channel creation process is presented here:

```
Process: Creation of the Communication Channels
if (delay > 0 || ber > 0 || datarate > 0)
          { channel =
cDatarateChannel::create("channel");
if (delay > 0)
               channel->setDelay(delay);
if (ber > 0)
               channel->setBitErrorRate(ber);
if (datarate > 0)
               channel->setDatarate(datarate);
     }
src->connectTo(dest, channel);
```

I. Attack Tracker

This component of the framework relies on the characteristics of the attacks and identifies the presence of attacks in the network. The characteristic based attack detection rule engine is presented here [Table – II].

Table II: Attach Characteristics Rule Set

Attack Type	Rule Formulation
Interrogation	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:Yes,Dead Node:No
Energy Drain	Energy:Yes,Delay:Yes,Routing Pattern:No,High Traffic:Yes,Dead Node:Yes
Hello Flood	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:No,Dead Node:No
Misdirection	Energy:No,Delay:Yes,Routing Pattern:No,High Traffic:No,Dead Node:No
Flooding	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:No,Dead Node:No
Jamming	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:No,Dead Node:No
Collision	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:No,Dead Node:No
Black Hole	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:Yes,Dead Node:No
Denial of Service	Energy:Yes,Delay:Yes,Routing Pattern:No,High Traffic:Yes,Dead Node:Yes
Selective Forwardin g	Energy:No,Delay:No,Routing Pattern:Yes,High Traffic:No,Dead Node:No

Hence, these rule sets decides the presence of the attacks on the network can informs the trust manager to exclude the node.

J. Performance Comparator

The final component of the framework is the performance comparator. The details of the parameters are listed here [Table –III].

Table III: Performance Comparator Framework

Parameter Name	Parameter Description
Computational Cost	The computation of the number of iterations for trust management and the time
Key Sharing Time	The time taken for key sharing by the trust manager
Multi-Channel Selection Time	Time taken for the communication channel selection and the time for random number generation
Over-all network time complexity	The total time for transmitting the data packet
Attack Detection ratio	The ratio between number of attacks detected and the attacks encounters

In the next section of the work, the results obtained from this framework are elaborated and discussed.

II. RESULTS AND DISCUSSIONS

The results obtained from this proposed framework are highly satisfactory. This section of the work, discusses the results of the proposed framework based on computation time or computational cost, key sharing time, multi-channel selection time with the outcomes and finally the effects of the attacks and the detection ratio.

A. Computational Cost

Firstly, the computational cost for the trust manager is observed for this model. The findings are listed here in [Table –IV].

Table IV: Computational Cost

Sequence ID	Event Type	Time (ns)
#1	cMessage - TM	0.107635108
#4	cMessage - TM	0.107667876
#8	cMessage - TM	0.107800644
#12	cMessage - TM	0.107933412
#16	cMessage - TM	0.175913545
#19	cMessage - TM	0.175946313
#23	cMessage - TM	0.176079081
#27	cMessage - TM	0.224590518
#30	cMessage - TM	0.224623286

The findings are visualized graphically here in [Fig – 7].

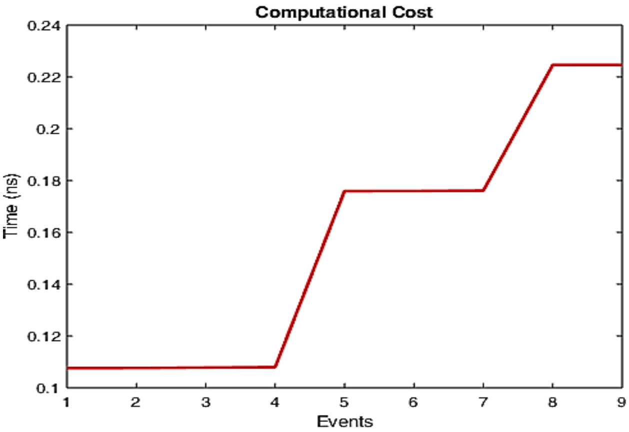


Fig. 7 Computational Cost of the Trust Management

B. Key Sharing

Secondly, the key sharing time complexity is observed and the findings are listed here in [Table – V].

Table V: Key Sharing Time Complexity

Event Type	Trust manager Random Number	Time (sec)
Packet_Transmit_Start	1	0.03
Packet_Receive_Start	8	0.03
Packet_Receive_Start	9	0.03
Packet_Receive_Start	10	0.03
Packet_Receive_Start	11	0.03
Packet_Receive_Start	12	0.03
Packet_Receive_Start	13	0.03
Packet_Received	12	0.06
Packet_Received	13	0.06
Packet_Received	14	0.06
Packet_Received	23	0.06
Packet_Received	24	0.06
Packet_Receive_End	8	0.06
Packet_Receive_End	9	0.06
Packet_Receive_End	10	0.06
Packet_Receive_End	11	0.06
Packet_Receive_End	12	0.06

Thus it is natural to understand that the using the random numbers are trustable for normality and randomness in distributions.

C. Multi-Channel Selection

Thirdly, the multi-channel selection algorithm results are identified and illustrated for observation in [Table – VI].

Table VI: Multi-Channel Selection

Event Type	Selected Channel	Time (sec)
Channel_Request	1	0.03
Channel_Idle_Check	1	0.03
Channel_Idle_Check	0	0.07
Channel_Idle_Check	0	0.07
Channel_Idle_Check	0	0.07

Channel_Idle_Check	0	0.07
Channel_Idle_Check	1	0.07
Channel_Idle_Check	0	0.07
Channel_Idle_Check	0	0.07
Channel_Idle_Check	1	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	1	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	0	0.08
Channel_Idle_Check	1	0.08
Channel_Idle_Check	0	0.08

The result is visualized graphically here in [Fig – 8].

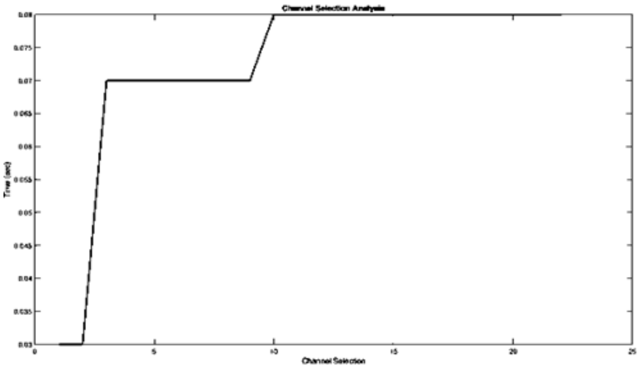


Fig. 8 Channel Selection Time Complexity

D. Effect of Attacks or Attack Detection Ratio

Fourthly, a number of attacks were simulated on the proposed framework and the detection findings are also listed here in [Table – VII].

Table VII: Attack Detection

Test Sequence	Attack Types	Detection Status
Test - 1	Collision	Yes
Test - 2	Selective Forwarding	Yes
Test - 3	Denial of Service	No
Test - 4	Energy Drain	No
Test - 5	Denial of Service	No
Test - 6	Interrogation	Yes
Test - 7	Selective Forwarding	Yes
Test - 8	Flooding	Yes
Test - 9	Misdirection	Yes
Test - 10	Collision	Yes
Test - 11	Black Hole	Yes
Test - 12	Energy Drain	No
Test - 13	Hello Flood	Yes
Test - 14	Interrogation	Yes
Test - 15	Jamming	Yes
Test - 16	Jamming	Yes
Test - 17	Flooding	Yes
Test - 18	Black Hole	Yes
Test - 19	Misdirection	Yes
Test - 20	Hello Flood	Yes

Hence, it is natural to observe the statistical analysis of the findings in [Table – VIII].

Table VIII: Attack Detection Ratio

Parameters	Norm
Number of Tests	20
Number of Attack types	10
Number of Attacks	20
Number of Attacks detected	16
Attack Detection	80%

Hence, it is natural to realize that nearly 80% of the attacks can be detected in this framework.

E. Packet Delivery Analysis

Finally, the packet delivery analysis is presented here in [Table – IX].

TABLE IX: Packet Delivery

Event Sequence	Event Type	Time **(sec)**	Packet Delivery Success
#2	Packet_Delievery	0.107635108	Yes
#3	Packet_Delievery	0.107635108	Yes
#5	Packet_Delievery	0.107767876	Yes
#6	Packet_Delievery	0.107767876	Yes
#7	Packet_Delievery	0.107767876	Yes
#9	Packet_Delievery	0.107900644	Yes
#10	Packet_Delievery	0.107900644	Yes
#11	Packet_Delievery	0.107900644	Yes
#13	Packet_Delievery	0.108033412	Yes
#14	Packet_Delievery	0.108033412	Yes
#15	Packet_Delievery	0.108033412	Yes
#17	Packet_Delievery	0.175913545	Yes
#18	Packet_Delievery	0.175913545	Yes
#21	Packet_Delievery	0.176046313	Yes
#22	Packet_Delievery	0.176046313	Yes
#24	Packet_Delievery	0.176179081	Yes
#25	Packet_Delievery	0.176179081	Yes
#26	Packet_Delievery	0.176179081	Yes
#28	Packet_Delievery	0.224590518	No
#29	Packet_Delievery	0.224590518	No

The time for packet delivery is visualized here [Fig – 9].

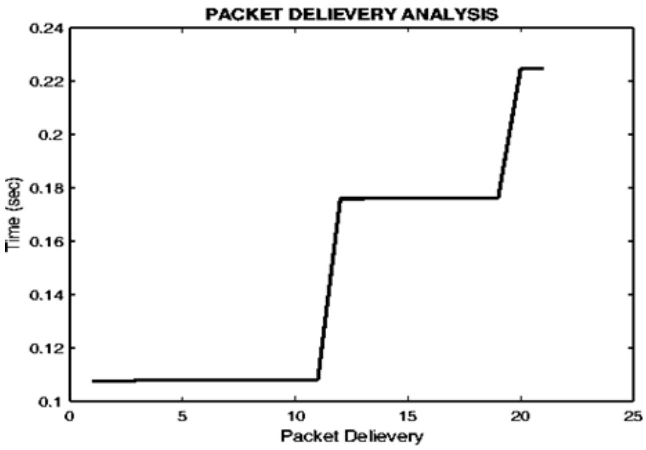


Fig. 9 Packet Delivery Time Complexity

Further, the statically analysis is carried out on the findings [Table –X].

Table X: Packet Delivery Ratio

Parameters	Norm
Number of Iterations	22
Number of Packets Sent	22
Number of Packets Received	20
Average Packet Delivery Time (Sec)	0.1449
Packet Delivery Ratio	90.9%

F. Comparative Analysis

In order to establish the improvement over this proposed scheme for routing, the comparative analysis is presented here. This section of the work analyses the existing algorithms and compares with the proposed algorithm for secure routing based on standard metric for performance evaluation [Table XI]. Based on the analysis, the algorithms are ranked as well.

Table XI: Comparative Analysis [26]

Name of the Scheme	Scalability	Delay in Transmission	Node Distributions	Control Message	Energy Consumption	Algorithm Complexity	Ranking
LEACH	Low	Low	Random	No	Low	Low	11
LEACH – C	Low	Low	Random	No	Moderate	Low	5
PEGASIS	Low	Low	Random	No	Moderate	Low	4
TEEN	Low	Low	Random	No	Low	Low	3
CCS	Moderate	Low	Random	No	Moderate	Moderate	6
EBCRP	Moderate	High	Random	No	Moderate	Moderate	7
CHIRON	Moderate	Low	Random	No	Moderate	Moderate	8
EADTR	Moderate	High	Random	No	Moderate	Moderate	9
PEDAP	Moderate	High	Random	Yes	Low	Moderate	10
ETR	High	Low	Random	Yes	High	Moderate	2
Proposed MOSDCB	High	Low	Random	Trust Based	High	High	1

Thus, it is natural to realize that, the proposed MoSDCB algorithm for secure routing is significantly better in comparison with other parallel outcomes.

III. CONCLUSION

The wide use of wireless sensor networks for various critical information sharing purposes makes the domain highly adopted for research. A number of attempts for securing the routing scheme without tampering the low cost implementation, flexible structure, low energy consumptions are carried out. The most popular being the trust based management schemes are also not guaranteed to be secure. Thus the demand for enhancements continued to persist. The major drawback of the trust based systems is provocation of the newer types of attacks. The trust based schemes are easy to guess and that makes the policies vulnerable to attacks. Thus, the proposed multi order key sharing with dual channel based secure routing protocol has been established. The proposed scheme demonstrates high packet delivery ratio with benefits from majority of the attacks. This work is proven to be a newer direction of research in order to fulfil the demand of secure routing for a worldwide secure communication.

REFERENCES

1. O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener,``Transmission with energy harvesting nodes in fading wireless channels: Optimal policies,'' IEEE J. Sel. Areas Commun., vol. 29, no. 8, pp. 17321743, Sep. 2011.
2. N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, ``Active low intrusion hybrid monitor for wireless sensor networks,'' Sensors, vol. 15, no. 3, pp. 2392723952, 2015.
3. G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, ``Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply,'' IEEE Trans. Power Electron., vol. 17, no. 5, pp. 669676, Sep. 2002.
4. A. K. A. Mohammad and S. Gadadhar, ``Enhancing cooperation in MANET using neighborhood compressive sensing model,'' Egyptian Informat. J., vol. 6, no. 1, pp. 115, 2016.
5. G. G. Uttam and D. Raja, ``SDRP: Secure and dynamic routing protocol for mobile ad-hoc networks,'' IET Netw., vol. 3, no. 2, pp. 235243, 2014.
6. W. K. K. Chin and K. L. A. Yau, ``Trust and reputation scheme for clustering in cognitive radio networks,'' in Proc. Int. Conf. Frontiers Commun.,Netw. Appl. (ICFCNA), Kuala Lumpur, Malaysia, Nov. 2014.
7. Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, ``A novel energy aware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment,'' Sensors, vol. 15, no. 10, pp. 3110831124, 2015.
8. J.G. Choi and S. Bahk, ``Cell-throughput analysis of the proportional fair scheduler in the single-cell environment,'' IEEE Trans. Veh. Technol.,vol. 56, no. 2, pp. 766778, Mar. 2007.
9. K. B. Sourav and M. K. Pabitra, ``SIR: A secure and intelligent routing protocol for vehicular ad hoc network,'' IET Netw., vol. 4, no. 6, pp. 185194, 2015.
10. E. Adel, K. Abdellatif, and E. Mohammed, ``A new trust model to secure routing protocols against DoS attacks in MANETs,'' in Proc. 10th Int. Conf. Intell. Syst. Theories Appl. (SITA), Taipei, Taiwan, Oct. 2015, pp. 16.

11. J.M. Chang, T. Po-Chun,W. G. Isaac, C. C. Han, and C. F. Lai, ``Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Syst. J., vol. 9, no. 6, pp. 6575,Jun. 2015.
12. P. G. Fernando, M. C. A. Rossana, T. O. Carina, and J. N. Souza,``EPMOSt: An energy-efcient passive monitoring system for wireles ssensor networks," Sensors, vol. 14, no. 3, pp. 1080410828, 2015.
13. X. Du and H. H. Chen, ``Security in wireless sensor networks," IEEE Wireless Commun., vol. 15, no. 4, pp. 6066, Aug. 2008.
14. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ``A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J., 2017.
15. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, ``Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," Int. J. Netw. Secur., vol. 5, no. 9, pp. 1421, 2007.
16. D. Zhu, X. Yang, W. Yu, and X. Fu, ``Network coding vs. Traditional routing in adversarial wireless networks," Int. J. Ad Hoc Netw., vol. 20, no. 2, pp. 119131, 2014.
17. P. Zhao, X. Yang, W. Yu, and X. Fu, ``A loose virtual clustering based routing for power heterogeneous MANETs," IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 22902302, Sep. 2013.
18. W. Yu and J. Lee, ``Efcient energy sensitive routing protocols in mobile ad-hoc networks," in Proc. Process. Int. Conf. Wireless Netw., Shanghai,China, Jun. 2002, pp. 39.
19. R. Morsi, D. S. Michalopoulos, and R. Schober, ``Multiuser scheduling schemes for simultaneous wireless information and power transfer over fading channels," IEEE Trans. Wireless Commun., vol. 14, no. 4, pp. 19501964, Apr. 2015.
20. J. Yao, S. Feng, X. Zhou, and Y. Liu, ``Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," IEEE Trans. Commun., vol. 64, no. 2, pp. 753764, Feb. 2016.
21. B. Paramasivan, M. J. V. Prakash, and M. Kaliappan, ``Development of a secure routing protocol using game theory model in mobile ad hoc networks," J. Commun. Netw., vol. 17, no. 1, pp. 7583, Feb. 2015.
22. I. Krikidis, S. Timotheou, S. Nikolaou, and G. Zheng, ``Simultaneous wireless information and power transfer in modern communication systems,"IEEE Commun. Mag., vol. 52, no. 11, pp. 1642416450, Nov. 2014.
23. A. Vosoughi, R. C. Joseph, and A. Marshall, ``Trust-aware consensusinspired distributed cooperative spectrum sensing for cognitive radio adhoc networks," IEEE Trans. Cognit. Commun. Netw., vol. 2, no. 3,pp. 2437, Sep. 2016.
24. A. Cornejo, S. Viqar, and J. L. Welch, ``Reliable neighbor discovery for mobile ad hoc networks," Ad Hoc Netw., vol. 12, no. 6, pp. 259277, 2014.
25. Y. Sun, Z. Han, and K. J. R. Liu, ``Defense of trust management vulnerabilities in distributed networks," IEEE J. Mag., vol. 46, no. 2, pp. 112-119,Feb. 2008.
26. Anuj Kumar Singh ; Anshika Bhalla ; Pramod Kumar ; Manju Kaushik, Hierarchical routing protocols in WSN: A brief survey, (ICACCA) (Fall), 2017 3rd International Conference on, April 2018.