Secure Trust Aware Hybrid Key Management Routing Protocol for WSNs for the Application of IoT

Sharmila, Kumkum Som, Umang Kant, Pramod Kumar

Abstract*: Secure Trust Based Key Management Framework for Wireless Sensor Networks (WSNs) to protect the forwarded packets from intermediary malicious nodes. The proposed method continuously ensures the trustworthiness of cluster heads by replacing them as soon as they become malicious and can dynamically update the packet path to avoid malicious routes. Unlike the other methods, the process is distributed among the nodes to minimize routing overhead and to conserve energy. The fundamental process of moving node to non-switchable Low Power Listening (LPL) state assists energy conservation. Trust based neighbor selection is carried out using Gateway node (GW) and Monitoring Node (MN) monitors other node activities so as to ensure security in the network. The manifold process integrated improves network performance in terms of throughput, retaining network lifetime and conserving energy utilization at midst the presence of adversary nodes. The proposed method can significantly outperforms traditional cluster based routing protocols that do not use trust concept in selecting the forwarding nodes in packet delivery ratio. Comparisons and analysis have shown the effectiveness of the proposed scheme.

Keywords—listening, routing, sensor nodes, trust, power.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) comprises of self-operating motes that are deployed to support wide applications in real world. Sensor nodes are more vulnerable to attacks. A common method for ensuring reliability is that the nodes must rely on their neighbors. In other words, the nodes trust their neighbors for routing and transmission irrespective of the area of their deployment. Sensor network incorporates both good and false nodes; selecting good sensor nodes needs a better processing. A node expects the co-operation of its neighbor to perform the network operations; without complete knowledge of its neighbor that turns out to be vulnerable. Therefore it is necessary for a node to select secure / trusted neighbor as recommended by it or other neighbors. Most of the trust management system collects feedback from malicious node in the network. It produces incorrect trust value. Though, most of the previous studies have not addressed the issue of feedback from malicious nodes which affects the system dependability and feedback availability; it may result in inaccuracy of the trust. These limitations cause route misdirection attack. This attack can be overcome by means of using authentication and monitoring the sensor nodes in the network. The solutions proposed so far is to improve network performance in the earlier stage of the network operations only. In the post operation, energy constraints are not considered which increase routing overhead.

To ensure safe routing path, the proposed Trust aware Hybrid Key Management routing protocol (THKP) establishes dedicated path through trusted nodes with help of key management scheme. The proposed protocol forwards packets through trusted nodes only and identifies the malicious nodes based on the behavior and forms new route to detour from them. The proposed Secure Trust Aware Hybrid Key Management based routing protocol for WSNs is based on key management and trust which provides an energy optimization and overhead control.

II. LITERATURE SURVEY

Wireless Sensor Networks is a form of Ad-Hoc Network that employs routing protocols for network operations like route discovery and broadcast. Routing protocols can be either reactive or proactive [13] . Proactive protocols maintain the neighbor information all time in an updated manner; the reactive protocols learn about the neighbors when source requires relaying [14]. The protocols defined for routing contain least security features that do not withstand a complex vulnerability. Therefore, researchers have developed security incorporated routing protocols that support security routing. [15]

Aravindh et.al.,[17] proposed Trust and Energy aware Routing Protocol (TERP) to balance energy consumption of the network and trustworthiness of the nodes, in an effective manner. TERP identifies and discards bad nodes so as to provide security whereas the energy aware characteristic of the protocol distributes the network load with the prior knowledge of the energy available with the nodes. TERP sustains in handling network load over an improved network lifetime.

Revised Manuscript Received on July 10, 2019

Dr. Sharmila, Department of CSE, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India
Kumkum Som, Department of CSE, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India
Umang Kant, Department of CSE, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India
Dr.Pramod Kumar, Department of CSE, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India

Marchang and Datta [13] proposed a Light weight Trust Based routing protocol, LTB-AODV to improve network throughput and packet delivery ratio with lesser packet drop. The authors modified Adhoc On demand Distance Vector (AODV) to select trusted neighbors instead of selecting the shortest path neighbors (traditional approach).

The trusted neighbors are identified using local information and also utilized path trust for selecting nodes in the network. This method is not scalable for large networks where multiple verification and trust computation methods are necessary. Ahmed and Bakar et. al., [11] proposed a variant called Trust and Energy Secure Routing Protocol (TESRP) in which node selection is carried out based on: trust value, enduring energy of the node and number of hops to the neighbors. Apart from distributing load, this variant is intended to improve network life span and throughput by conserving energy utilization. A Secure Trust based Key Management Framework (STKF) to improve data delivery and security is proposed by the authors Kaur and Gill[12]. STKF selects neighbors based on trust values with distance as it threshold factor. STKF is a resistant to internal attacks by replacing malicious nodes with good nodes. Post replacement and STKF intends nodes are used to create a dedicated path for transmission discarding the previously built path.

A. Limitations of Existing Trust Mechanism for WSNs

The following are the limitations imposed by the trust mechanism for WSNs,

- Most of the existing works are focused on the trustworthiness of clustered WSNs and they fail to address the problem of resource limitation of nodes complex algorithms which are used to estimate node's trustworthiness.
- In real time applications, it is impractical to use complex trust algorithm at each cluster head or cluster member nodes. While periodically exchanging trust related information between the sensor nodes in large scale WSNs which leads to high communication and computational overhead.
- Furthermore, most of the work is focused on the remote feedback trust management systems which collect feedback from the nodes and aggregates the feedback to calculate the global trust degree of the node. Trust management system also collects feedback from malicious node in the network which produces incorrect trust value. Though, most of the previous studies do not address the issue of feedback from malicious nodes which affects the system dependability and feedback availability.
- These limitations cause route misdirection. Route misdirection is an attack whereby the mischievous node broadcast false trust values to either inject fake traffic into the network, direct traffic to a false node or reject part of network by draining its resources. This attack can be overcome by means of using authentication and monitoring the network. So, the security and trustworthiness of the cluster member and neighbor CHs play an important role to ensure the secure data transmission through the faithful route.

The main contribution of the proposed method is to overcome the above limitations and in order to ensure safe routing path, the proposed Trust aware Hybrid Key Management routing protocol (THKP) establishes dedicated path through trusted nodes with help of key management scheme. The proposed protocol forwards packets through trusted nodes only and identifies the malicious nodes based on the behavior and forms new route to detour from them. The proposed Secure Trust Aware Hybrid Key Management based routing protocol for WSNs is based on key management and trust which provides an energy optimization and overhead control.

III. SECURE TRUST AWARE HYBRID KEY MANAGEMENT ROUTING PROTOCOL (THKP)

The proposed secure Trust aware Hybrid Key Management based on routing Protocol (THKP) which concentrates both on conserving energy to retain an appreciable count of alive nodes in the network and also security. Energy efficiency is achieved using Low Power Listening (LPL) and energy threshold. Security is achieved by selecting higher trust valued neighbors.

The process of THKP is illustrated in Fig.1.The proposed secure routing method selects an effective node that can sustain a prolonged transmission based on energy of the node. The trust of each selected node is computed and finally, few nodes are filtered to pursue transmission at that instance of time. The proposed THKP works in two phases namely Energy Constraint Selection and Trust Constraint Selection.

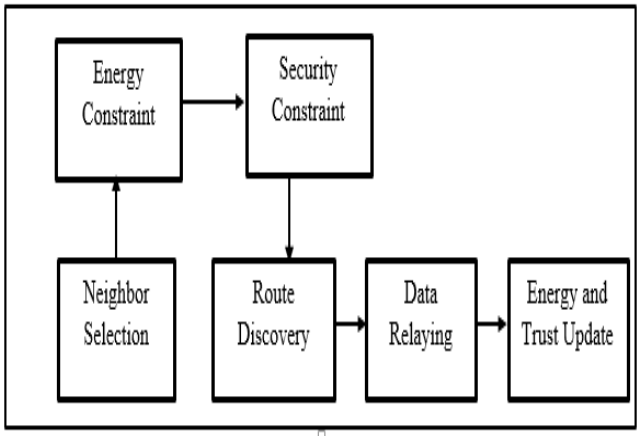

Fig. 1 Process of THKP

A. Network Scenario

Cluster based WSNs (CWSNs) is considered which consists of {1,2,..,n} set of nodes that belong to N, where N is number of sensor nodes in the network. The nodes are randomly dispersed in the network with periodic peer-peer-trust evaluation as the security metric. Node 'i' and 'j' are said to be direct neighbors for a cluster head (CH) provided the nodes are in range of CH. Each cluster consists of a gateway node (GW) and Monitoring Node (MN) for communication and trust verification.

The monitoring node (MN) verifies the consistency of GW. Authenticated node in the Cluster Head (CH) is chosen as a monitoring node based on Hybrid Key Management Scheme (HKMS).

Each node in the network maintains a routing table that maintains the neighboring information and filtering record that hold the condition specific information of the relaying nodes.

B. Energy Model

Let E_i represent the pioneer (initial) energy of the node. A node utilizes its energy for routing the data packets. Energy utilized by a node (E_u) varies as the distance to the aggregator varies. If E_t and E_r represent the energy consumed by a node for transmitting and receiving data respectively, then by [14]

$$E_u = E_t + E_r \quad (1)$$

To prevent the nodes being active all time, node which do not perform transmission are made to power off their radio transmitter with their radio receiver alone kept in ON state. The node utilizes only lesser amount of energy to listen broadcast directed towards it. This state is called Low-Power-Listening (LPL).

E_t and E_r can be computed using equation (2) and (3) respectively.

$$E_t = d_t \times e_t \times t_t \quad (2)$$

Where, d_t is the data transfer rate, e_t is the transmission energy and t_t is the data transfer time.

$$E_r = d_r \times e_r \times t_r \quad (3)$$

Where, d_r is the data reception rate, e_r is the reception energy and t_r is the data reception time.

C. Energy Constraint Selection

In energy constraint based neighbor selection, the nodes are selected based on their enduring (residual) energy. The node with higher enduring energy is prefer for routing. The active transmitting node collects the information of all the higher enduring nodes and stores the information. The path discovering node discards the node whose energy has reached the threshold level (E_{th}). The threshold energy level is defined as the half drain energy of the sensor node. The half drain (E_h) of the sensor node is computed using,

$$E_h = \frac{E_i}{2} \quad (4)$$

Where E_i is initial energy of sensor nodes. Therefore it is necessary that each node has to be monitored for its enduring energy post of each set of transmission. The enduring energy (E_R) of the node is given by equation (5)

$$E_R = E_i - E_u \quad (5)$$

where E_u is used energy of sensor nodes.

The neighbor selecting nodes creates a list (a_f) for the set of forwarders that are capable of transmitting data.

$$a_f = \{1,2,3,\dots,i\}$$

The rest of the nodes are moved to LPL state which is otherwise termed as leisure state. Unlike in duty cycle process, the nodes are not switched between the states frequently. The nodes that reach their half drain level are replaced with the nodes in LPL states. To minimize the overhead in selecting neighbors using non-periodic control messages, it prevents integration of duty cycle process. The nodes in LPL (i_f) are represented as,

$i_f = \{1,2,3,\dots,j\} \in n$, where $i \neq j$ and $i,j \in N$ where N is number of sensor nodes in the network. The nodes in a_f will satisfy the below condition:

$$a_f = \max\{1,2,3,\dots,n\} \in N$$

D. Trust Constraint

Trust constraint converges the neighbor energy efficiency towards security in the process of neighbor selection. The nodes that are in a_f are checked for their trust, after each transmission along with the energy level. Among the nodes in a_f, a set of nodes are further filtered to pursue transmission, by the GW. A monitoring node evaluates trust value of the gateway node based on the transmission history. A gateway node must update its transmission history to the monitoring node failing of which will be declared as un-trusted node. Monitoring Node verifies the transmission history of the GN with the transmission information fetched from the CH. MN computes the Packet Transmission Factor (PTF) of GN.

The trust value computed over the CH and the GW to determine the node's participation in routing. Trust computation is considered in three possible ways:

i. ***Direct Trust (DT):*** In a direct trust, the nodes that are in communication range of their neighbors compute each other's trust and update the same to their ancestors.

ii. In-Direct Trust (IT): The forwarding nodes request their one-hop neighbors to compute the trust of their promoting nodes. The requesting nodes accept the trust as given by their direct neighbors.

iii. Path Trust (PT): Both through direct or indirect trust, the mean of each path is computed and the transmitting node is considered as multiple path trust values in selecting its neighbor.

As the enduring energy of each one-hop node is considered for effective neighbor selection which avoids indirect trust and path trust to prevent unnecessary update. The direct trust between CH and GW (dt_{ch-gw}) is computed by MN [15] [18] using equation (6)

$$dt_{ch-gw} = \frac{tp_{ch}}{rp_{gw}} \quad (6)$$

Where, tp_{ch} is the packets transmitted from Cluster Head and rp_{gw} is the count of packets received by gateway node.

The trust of all one-hop nodes need to be considered for selection, where $(i,j) \in a_f$. The trust factor computed by MN and energy of the selected node will be updated for each transmission. With reference to the enduring energy, based on trust, the nodes need to be changed frequently. As in energy, trust also needs a threshold value for evaluating nodes' trust.

The threshold value (θ) for node [15] is computed using equation (7)

$$\theta = \frac{\omega_n}{\omega_{n-1}} \quad (7)$$

where ω_n is the number of links or connections associated with a node the gateway node.

$$w_n(t) = \{l_{i,j} \epsilon N : E_{d_t}(j,k) \leq R\} \quad (8)$$

where $l_{i,j}$ is a link between node CH (i) and gateway node (j), E_{d_t} is a link between connecting destination at time t and R is a transmission range

Node's trust value is greater than θ which is selected for routing by its previous neighbor. The number of node changes for energy and trust need not be the same. This is because node energy drain requires multiple routing trust update. When the number of active nodes is large in number, the proposed trust based model can prevent unnecessary broadcast and control message overhead by minimizing the selection condition based on packet drop.

If p_s and p_d denote packets that are successfully transmitted and dropped, respectively, then we consider two cases for node selection.

Case 1: if $p_s > p_d$ then, equation (6) can be rewritten as in equation (9).

$$dt_{i,j} = ct_{i,j} + \left(\frac{1-ct_{ij}}{\omega_n}\right) \quad (9)$$

Case 2: if $p_s \leq p_d$ then, equation (6) can be rewritten as in equation (10).

$$dt_{i,j} = ct_{i,j} + \left(\frac{1-ct_{ij}}{\Delta t}\right) \quad (10)$$

Where, $ct_{i,j}$ is the current trust value computed by node 'i' over 'j' and Δt is the interval of time taken to compute the current trust. Fig.2 describes unanimous trusted neighbor selection.

Trusted Neighbor Selection

Step1: for all $n \in a_f$ in $X * Y$ {
Step2: Get sp, rp
Step3: Compute direct trust as $dt(CH-GW) = \frac{sp}{rp}$
Step4:if{$dt(GW) > dt(GW+1)$ && $dt(GW) > \theta$}
Step5: { routing node= GW
Step6: else
Step7: routing node GW+1
Step8: } end if
Step9: Initiate RREQ to GW
Step10: Get RREP from GW
Step11: } end for

Fig. 2 Trusted neighbor selection algorithm

E. References

The transmitting node initiates broadcast message to all the nodes available in its range. The neighbours reply back with their current energy level and trust. MN monitors all the information broadcasted by the neighbours. Transmitting node on receiving the energy level of each node, sorts the node IDs in descending order of their enduring energy. The node declares the sorted list as active forwarders a_f. The other nodes discarded for energy constraint will be used in the next routing cycle. To confirm neighbour selection, the transmitting node further verifies the trust value of the GW with the MN.

The transmitting node initiates Route Request (RREQ) through the higher trust GW present in its range. The GW forwards the RREQ to the sink node through a series of forwarders selected in the same manner. The sink node on receiving the RREQ acknowledges with a Route Reply (RREP) that is received by the transmitting node through the same set of neighbors, through the GW.

Packet Received	Packet Forwarded	Drop Count	Time	Remaining Energy	Trust Value

Table 1 - Transmission Information Table Representation.

Transmitting node confirms the path using RREQ and RREP messages for transmission. After each transmission, the current trust nodes that belong to a_f are checked for their transmission status. MN maintains transmission information of the nodes as shown in Table. 1.
Each node shares the table information with its pre-hop neighbor and the neighbor computes the trust using equation (6). Source node verifies, if the number of trust assigned nodes is equal to the node degree i.e.

$$\textbf{Count (trust assigned)} = \omega_n$$

The trust of each node is updated by its pre-hop neighbor. Similarly the remaining energy of the node is updated using equation (5). Fig.3. provides an algorithm for neighbor selection with energy efficiency is given below.

Energy Efficient Neighbour Selection

Step1: for all $GW \in CH$ in $X * Y$ {
Step2: Initiate broadcast(SID, DID)
Step3: if{$d(GW) \leq t_r(S)$} {
Step4: Get $E_R(GW)$

$$E_R(GW) = E_i(GW) - E_u(GW)$$

Step5: Compute E_h for all GW nodes

$$E_h(GW) = \frac{E_i(n)}{z}$$

Step6: if{$E_R(GW) > E_h(GW)$} {
Step7: $\{a_f\} \leftarrow : E_R(GW)$
Step8: $\{a_f\} = descend\_sort\{a_f\}$
Step9: } end if
Step10: } end if
Step11: } end for

Fig. 3 Energy efficient neighbor selection algorithm

Table 2 provides a description about the acronyms used in the algorithms

Symbol/ Acronym	Description
d(GW)	Distance to the GW node
$t_r(S)$	Transmission Range of source
GW	Current Gateway node
GW+1	Next Gateway node

Table 2 - Acronyms and its Description.

A node is discarded by MN based on the following conditions:
(i) If the GN does not share its transmission information with MN
(ii) If the enduring energy of the GN has attained the half dead state
(iii) The trust value of the GN is below threshold
(iv) The trust count and GN degree does not match with each other.
(v) GW transmission history and CH transmission information have disparity.

IV. METRICS FOR NETWORK PERFORMANCE ASSESSMENTS

A. Throughput

Throughput is defined as the total number of data packets/ bytes transferred during the simulation. Mathematically, throughput can be illustrated as

Throughput= (number of packets transferred * packet size)/ time

B. End-to-End Delay

Delay is the time taken for the data packets to arrive at the destination. Delay includes queuing time, buffering time, retransmission time, and latency in routing. Usually delay is represented as the difference between transmission time from source and arrival time at the destination.

Delay= Sum of (Processing delay, transmission delay, queuing and propagation delay)

C. Routing Overhead

Routing and data packets utilize the same bandwidth in the network, more frequently. Routing packets (Control messages) are considered to be a hindrance for data packets in the network. This possibility is called Routing Overhead. Routing overhead is defined in terms of number of control messages that are to be sent for route discovery and route maintenance to send data packets.

Routing overhead = (total packet size of control messages)/ (total packet size of data messages)

D. Energy consumption

Energy consumption is the amount of energy spent by a node for transmitting and receiving data over a time period.

Energy Consumption= Sum of (Transmission energy, Reception Energy)

E. Network Lifetime

Network lifetime is the time at which the first dead node occurs in the network as a result of exhausting its energy towards communication

V. METRICS FOR NETWORK PERFORMANCE ASSESSMENTS

The evaluation of the discussed parameters is aided with Network Simulator tool with a scenario of 1000X1000 dimensions. The simulation consists of 100 nodes that are densely populated with an initial energy for communication. The simulation parameters are charted in Table 3.The proposed THKP is compared with TERP [2][10] and LTB-AODV [13] for the above discussed metrics. The performance values are tabulated in Table 4.

Table 3 - Simulation parameters and its values.

Simulation Parameter	Value
Network Region	1000mX1000m
Nodes count	100
IEEE Standard	802.11
Transmission Range	250m
MAC	802.11
Initial Node Energy	20J
LPL Energy	4% of Initial Energy
Simulation Time	20s

A. Throughput

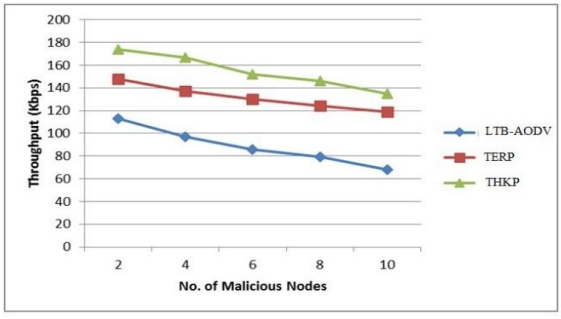

Fig. 4 Throughput Comparison between LTB-AODV, TERP and THKP

Fig.4. illustrates the throughput comparisons between the proposed THKP and existing LTB-AODV and TERP. From the simulation result, it is inferred that the proposed protocol secures the transmission by selecting trusted neighbors that are authenticated using hybrid key routing process. This ensures secure path availability that is less exposed to vulnerability. Therefore, the number of packets dropped is less, retaining a maximum throughput compared to the existing approaches.

B. Delay

Fig.5. shows the delay comparisons between LTB-AODV, TERP and THKP. From the simulation result, it is inferred that the proposed THKP is exposed to less vulnerability, due to dual authentication process in transmission and routing due to which re-transmissions are less when compared to the other methods. As the number of retransmissions and neighbor discovery do not take much of the time, delay is less in THKP. The forwarder selection is governed by the gateway node that reduces the time consuming task of the transmitting node.

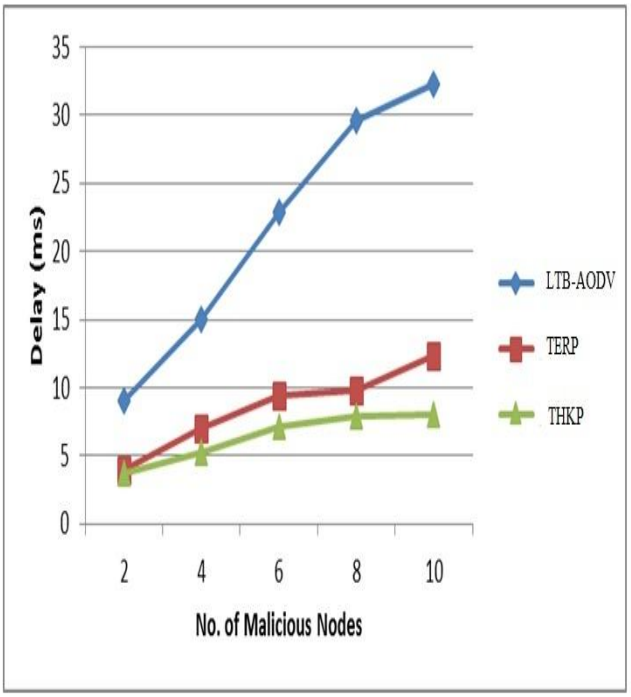

Fig.5. Delay Comparison between LTB-AODV, TERP and THKP

C. Routing Overhead

Fig.6. shows routing overhead comparison of proposed THKP with existing scheme. From the result, it is inferred that the proposed THKP avoids frequent neighbor selection as the link stability is ensured based on the secure neighbors availability. The periodic control message broadcast is minimized in THKP. Besides, the process of neighbor discovery is shared among GW and MN that aids forwarder selection with lesser broadcast. The co-operative nature of different functionality nodes help in minimizing the routing overhead in THKP, as compared to the existing protocols.

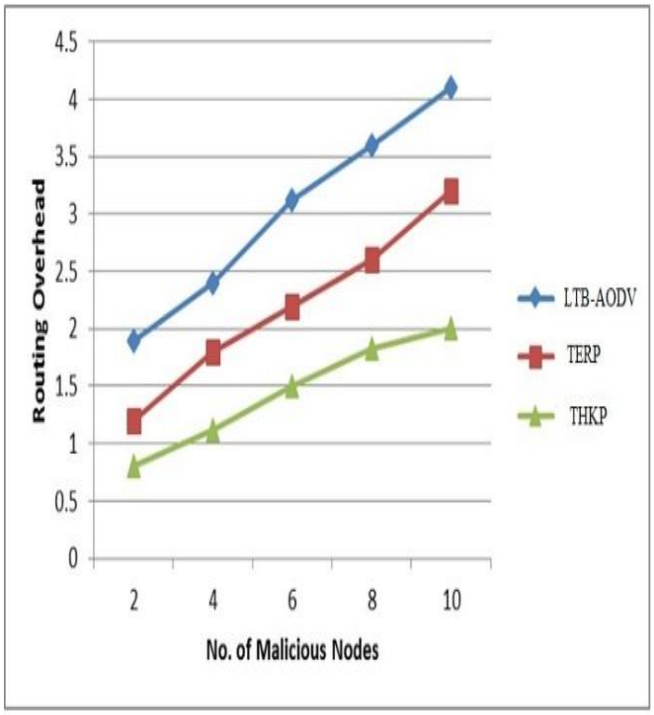

Fig.6. Routing Overhead Comparison between LTB-AODV, TERP and THKP

D. Energy Consumption

.

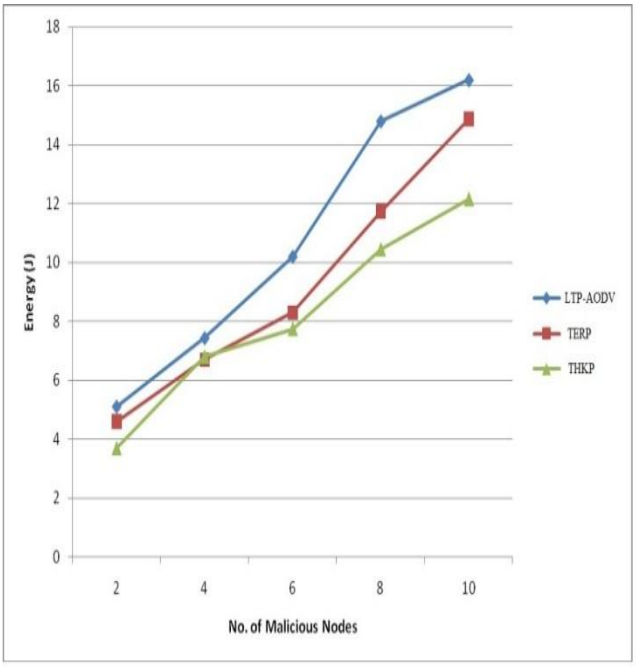

Fig.7. Energy Consumption Comparison between LTB-AODV, TERP and THKP

Energy consumption comparison between our proposed THKP and the existing LTB-AODV and TERP is shown in Fig.7.

Retrieval Number: I11150789S419/19©BEIESP
DOI:10.35940/ijitee.I1115.0789S419

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

From the simulation result, it is inferred that, the proposed THKP aids lesser energy consumption compared to the existing methods. Based on the fore hand information provided by MN and GW over node behavior and converged energy constraint neighbor selection schemes, an appreciable count of nodes remain in sleep state to minimize energy drain. The nodes' are swapped if they fail in the selection constraints, due to which the energy of all available nodes are not utilized most often.

E. Network Lifetime

Fig.8. shows the analysis of network lifetime for THKP, TERP and LTB-AODV. From the result, it is inferred that the proposed THKP retains node energy by preventing them being active all time which helps nodes that are not participating in routing to sustain their energy over a longer time than the other methods. Therefore over a series of transmissions, the transmission lasts for longer time, wherein a dead node occurs after prolonged communication. Therefore, THKP retains a maximum of the network lifetime compared to the other methods.

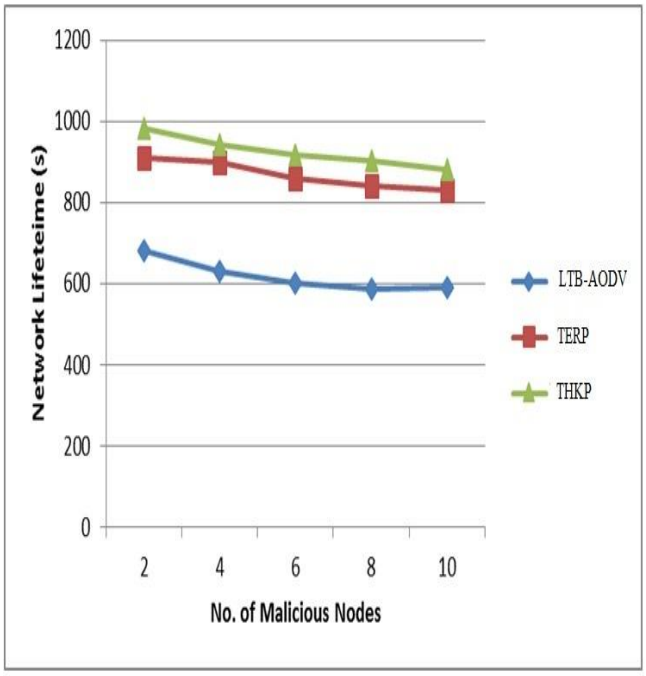

Fig.8. Network Lifetime Comparison between LTB-AODV, TERP and THKP

VI. CONCLUSION

A secure Trust based Hybrid Key Management Framework for WSNs was proposed in order to increase the performance of network in terms of energy consumption, throughput and network lifetime. The proposed THKP provides trust and energy efficient paths in resource constrained sensor networks. The throughput of the proposed scheme is 11% greater than the TERP scheme. The delay of the proposed TRP scheme 34.8% lesser than the existing scheme. The network lifetime of proposed method is 32.8% and 5.78 % greater than the LTB-AODV and TERP method. The PDR of proposed method is 12.7 % and 7.04 % greater than the existing method. It achieves improved performance in terms of energy consumption, throughput and network lifetime as compared to existing method.

REFERENCES

1. Royer, EM., & Toh, CK. (1999). A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, 6(2),1999, pp.46-55.
2. A, Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan.. A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Networks and Applications, 21(2) , 2016, 272–285.
3. J, Kaur, Gill, SS and Dhaliwal., "Secure trust based key management routing framework for wireless sensor networks," Journal of Engineering, vol. 2016, pp. 1–9.
4. Liu, K., Deng, J., Varshney, P.K., & Balakrishnan, K. , An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Transactions on Mobile Computing, 6(5), 2007, pp.536–550.
5. Sanzgiri, K., Dahill, B., Levine, BN., Shields, C., Belding-Royer, EM. A secure routing protocol for ad hoc networks, 10th International Conference on Network Protocols Proceedings, IEEE, 2002, pp. 78-87.
6. Ganeriwal, S., Balzano, L.K., & Srivastava, M.B. (2008). Reputation-based framework for high integrity sensor networks, ACM Transactions on Sensor Networks, 4(3), 2008, pp.1–37.
7. Bao, F., Chen, I.R., Chang, M., & Cho, J.H. . Hierarchical trust management for wireless sensor networks and its application to trust-based routing, Proceedings of the 2011 ACM Symposium on Applied Computing – SAC.
8. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A., ReTrust: attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, 16(4), 2012, pp.623–632.
9. Latha, D., & Palanivel. Secure routing through trusted nodes in wireless sensor networks–a survey," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2014, 3(8.).
10. Ahmed, A., Bakar, K.A., Channa, M.I., & Haseeb, K., &Khan.A.W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network, IEEE Sensors Journal, 15(12),2015, pp. 6962–6972.
11. Ahmed, A., Bakar, K.A., Channa, M.I., & Khan.A.W. A secure routing protocol with trust and energy awareness for wireless sensor network," Mobile Networks and Applications, 21(2), 2016, pp. 272–285.
12. Kaur, J., Gill, S.S., & Dhaliwal.B,S. Secure trust based key management routing framework for wireless sensor networks, Journal of Engineering, 2016, pp.1–9.
13. Marchang, N., & Datta.R., Light-weight trust-based routing protocol for mobile ad hoc networks, IET Information Security, 6(2), 2012, pp. 77-85.
14. Saraswat, J., & Bhattacharya, P. P. Effect of duty cycle on energy consumption in wireless sensor networks, International Journal of Computer Networks & Communications, 5(1), 2013, pp.120-125.
15. Sardar, M., & Majumder, K. "A new trust based secure routing scheme in MANET", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) Advances in Intelligent Systems and Computing, 2013, pp. 321-328.
16. Venkanna, U., & Velusamy, R. L. Mitigating the attacks on recommendation trust model for mobile ad hoc networks, International conference on Emerging Research in Computing , Information, Communication and Application (ERCICA), 2013, pp.123-130.
17. Aravindh, S., Vinoth, R. S., and Vijayan, R.(2013), A trust based approach for detection and isolation of malicious nodes in MANET", International Journal of Engineering and Technology (IJET),5(1), 2013, pp.193-199.
18. Jose, M.(2015), Trust management scheme in manet using uncertain reasoning and fuzzy logic in trust model, International Journal for Innovative Research in Science and Technology, 2(2), 2015, pp. 268-273.
19. Khan, M.S., Midi, D., Khan, M.I and Bertino, E.. Adaptive trust threshold strategy for misbehaving node detection and isolation", IEEE Trustcom/BigDataSE/ISPA, 1,2015, pp.718-725.