International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-13 Issue-01 April 2024
https://ijgst.com.2024.v13.i1.pp90-105

A Hybrid Secure Routing Mechanism in IoT-based Wireless Sensor Networks

E.ADINARAYANA [1] VENKATASUBRAMANYAMY [2] A SRIKANTH [3] CHALLA VINOD [4]
[1]ASSOC.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[3]ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[4] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract— The Internet of Things (IoT) has built its global pervasiveness for the planet Smart Networks Growth. It aims to deploy a network edge that helps IoT devices to use smart services and computing. In addition , in the event of any crises, this introduction will not only enhance the customer experience but also provide infrastructure stability. Edge computing utilises distributed architecture and end-user proximity in IoT applications to provide quicker response and improved service efficiency. However the question of protection is debated mainly to resist attacks' vulnerability (VoA). New technique senses intrusions in which the nodes of the sensors are spread to ensure a coherent manner with the sensor's static wireless network. Since sensor nodes are constantly in question across different transmission regions with multiple velocity levels, the choice of sensor monitoring nodes or guard nodes has become a difficult task in recent research. Furthermore, the adversaries often travel from one place to another to investigate their unique tasks across the network. We therefore suggest a stable routing and monitoring protocol with multi-variant tuples to provide scalable security using the symmetric key method of Two-Fish (TF) to discover and deter adversaries in the global sensor network. The proposed alternative is based on the ATE paradigm for Authentication and Encryption. With the Eligibility Weight Feature (ETF), the sensor guard nodes are chosen and concealed by complex symmetric key methods. By inheriting the properties of both Multipath Optimized Connection State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols, a stable hybrid routing protocol is selected to be constructed. Compared to the present routing systems, the outcome of the proposed solution reveals that it has a high number of monitoring nodes. In addition, the suggested routing mechanism is resilient to multiple mobile adversaries, ensuring multipath delivery.

Keywords— Things in Internet, wireless sensor networks; Symmetric key; Authentication and encoding model; Optimized routing connection status; Ad hoc on-demand vector multi-paths; Multipath distribution.

I. INTRODUCTION

As a third industrial revolution that integrates the electronic entity to transmit and retrieve physical data over the Internet, the IoT is generally accepted [1, 2]. It is a breathtaking-pace revolt that began with 2 billion physical objects in 2006 to 200 billion by 2020 [3], i.e. 200 percent rise.

In order to handle real-time activities that solve diverse problems, IoT devices / sensors typically capture and observe temporal / spatial data [4, 5]. For different uses, such as education, banking, energy , healthcare, transportation and smart cities[6], IoT applications are getting

smarter. Academia, industry and individuals are therefore struggling to provide security and security for IoT devices and networks.

In order to mitigate data disaster for IoT consumers, these variables should be primarily concerned. For eg, cyber-attackers can remotely control a smart home device and smart vehicle contact can be confiscated to establish a source of danger among people. In order to impact the IoT security structures and ecosystems of dynamic networking networks, such as social networks, apps, websites and Robo networks, i.e. botnet, this crisis scenario is highly exposed to Internet-connective artefacts. In comparison, the IoT-based device may be helpless as part or full network access by cooperating with a single communication channel or portion. Dyn cyber attack has gathers the communication device for installation and botnet collection in intelligent cities. By 2016 Zombie Army by Mirai recognized middleware. In addition to the flaws, attack vectors are now emerging in terms of variation and sophistication in the IoT framework.

Wireless Sensor Networks (WSN) is thus known to be a collection of services driving sensor nodes to gather atmosphere information, measure the gathered output into formatted information and send it to the destination terminal using the wireless media. Sensed information collected from different types of sensors, such as temperature, sensors for pressure, amplitude, level and flow and so on will be the source of input. In contrast to the tightly developed wired infrastructure networks, the open nature of the wireless medium makes the network vulnerable and defenceless to defend the data from adversaries. In war fields or defence-oriented applications, WSN[7] offers useful coordination to retrieve lights, electromagnetic signals, chemical or biological vapours, and enemy presence or boundary breaches. As nodes are in motion, supplying protection with optimised energy in WSNs is a tough task. In terms of defensive factors, the control of the localization of sensor nodes and travelling adversaries is the decisive one. There are various instances of attacks produced by opponents based on their interests or without any justification[8]. Any wireless sensor node fitted with enough hardware and software will act as an adversary to sense the wireless channel in an unauthorised way to collect the transmitting data. In addition, the opponents can attempt to modify the natural behavior of the usual sensor nodes and compromise it to breach the wireless sensor network operations, which will make the sensor nodes go downhill on their efficiency , performance, and service[9].

The Intrusion Detection System(IDS) is used in operation to deduce certain insecure events or attacks. In wired networks with the deployment of hardware systems between servers or nodes, IDS[10-12] is primarily used to track network operations. For the assessment of conventional network networks , i.e. not exclusively for IoT systems, IDS-based learning methods have been considered in the literature[13-18]. For network anomaly detection, Agarwal et al.[13] reviewed different data mining techniques. Buczak et al. [14] clarified the importance of cyberanalytics to survive infiltration and avoidance in data mining and machine learning techniques. In order to outline the problems of data defence, these study articles presented extensive references.

Fadlullah et al.[17] concentrated, however, on a deep learning mechanism for the study of traffic control systems. Hodo et al.[18] introduced the deep and swallow network taxonomy for intrusion detection and prevention systems surveys. In addition,

Wang and Jones [15] checked data mining, machine learning , deep learning, and bid-data to determine the parameters such as data streaming, encoding, reduction and function characteristics. The limits and restrictions of machine learning approaches to assess intrusion detection were compared and analysed by Mishra et al.[16]. The important notation utilised in this paper is shown in Table 1.

Table 1: Important Notation Used

Notation	Description
IoT	Internet of Things
VoA	Vulnerability of Attacks
TF	Two-Fish
ATE	Authentication and Encryption Model
EWF	Eligibility Weight Function
OLSR	Optimized Link State Routing (OLSR)
AOMDV	Ad hoc On-Demand Multipath Distance Vector
DSDV	Destination Sequenced Distance Vector
TARCS	Topology Change Aware-Based Routing Protocol
WSN	Wireless Sensor Networks
IDS	Intrusion Detection System
DIDS	Distributed Intrusion Detection System
BS	Base Station
CMS	Concealed Monitor Set
QoS	Quality of Services
DSR	Dynamic Routing Protocol
MANET	Mobile Ad hoc Network
VCG	Vickrey, Clarke, and Groves
MPR	Multipoint Relays
ANSN	Advertised Neighbor Sequence Number
ANIA	Advertised Neighbor Information Address
INITREQ	Initial Request
INITRES	Initial Response
MaRES	Mask Request
MaREQ	Mask Response
HMAC	Hash-based Message Authentication Code
PSQN	Packet Sequence Number
MAC	Medium Access Control
RCP	Routing Control Packets
PIT	Protocol Interface Table
SRT	Sandwiched Routing Table
CBR	Constant Bit Rate
UDP	User Datagram Protocol
DCF	Distributed Coordination Function

KMP	Knuth–Morris–Pratt

II RELATED WORKS

Generally speaking, in a broad variety of applications, wireless sensor networks(WSNs) are commonly used to provide responsive information. Data concealment is possible over free networking media to secure sensor nodes and network data, and has therefore been arbitrarily or hierarchically selected for adversarial detection.

A number of routing protocols have been suggested for ad-hoc mobile networks [19]. There is a specific application scenario and characteristics of each routing protocol. For eg, the Optimized Connection State Routing (OLSR) [20] protocol is well suited for high-density ad-hoc mobile networks, and the Destination Sequenced Distance Vector (DSDV) [21] protocol is desirable for ad-hoc small-scaling networks. When the implementation situation is complicated and the topology of the network differs quickly, a single routing protocol cannot ensure the mobility of the network to provide better performance.

An adaptive protocol for improved quality of services (QoS) has been created with correct environmental awareness and suitable approaches. In order to analyse communication metrics, Radhika Ranjan Roy [22] explained the mobility model. A range of mobility parameters were present in order to catch the essential characteristics, including geographical constraint, non-temporal and spatial dependence,[23]. The multiplicity of networks and topologies to decide network speed and efficiency have been identified by Hong et al.[24].

An expansion of the dynamic routing mechanism from DSR[19] that selects relative static nodes for the operation of aeronautical ad hoc networks[25]. Zheng et al.[26] proposed versatility and load-conscious routing for a merger of load sensing that finds the multispeed relay to minimise the average time-to-end.. Furthermore, high speed and unbalanced operating loads are applicable for unmanned aerial network. The Framework Model for describing three-layer mobility services for routing and mobility interactions was introduced by Bamis et al.[27].

In addition, for high-mobility networks of non-dense nodes, it is well equipped. In order to detect network congestion, Yu et al. [28] combined DSR routing with ant-colony optimization to stabilise signalling capacity.

In order to explore the paths, Swidana et al.[29] provided the basic concept of preventing a high-mobility node. Khalaf et al.[30] introduced a two-probability model to increase the speed of awareness that increases the ad-hoc on-demand routing performance of the network[31].

In order to solve the routing problem in multipath routing networks, Brahmbhatt et al.[32] proposed efficient routing that selects a strong node to stabilise signal frequency. Alejandro Proan and LoukasLazos[33] have concentrated on targeted jamming attacks that can be launched on the physical layer by real-time packet classification.

To have a good hiding commitment scheme, they have merged the symmetric key cryptographic schemes with physical-layer attributes. A wireless sensor network smart monitoring mechanism based on IEEE 802.15.4 Abderrezak Rachedi and Hend Baklouti have proposed MAC beacon-enabled technology[34]. The chief of the mobile ad hoc networks in presence of greedy intrusion detection nodes has been established two fundamentally

https://ijgst.com.2024.v13.i1.pp90-105

problematic[35]. To create the creation of trustworthy clusters with pre-distribution keys, a stable cluster formation algorithm [36] will be efficient.

III PROPOSED SYSTEM

Fig.1 illustrates the architecture of the proposed system. The sensed real time environmental variables are translated into a 'bt' bits set and distributed in time interval to other sensor nodes. The person or several transmitters may transfer their data to one or more destinations on these WSNs. As understood above, dense WSN, several constructive routing protocols are available to pick the right path for packets. But the particular protocol is not good for all the aspects like throughput, route discovery, link error identification and security scalabilities in congested wireless sensor networks. Reactive protocols handle survival routes efficiently, but they do not achieve low overhead for dense networks. As such, reactive protocols are overloaded with a persistent upgrading scenario and require maximum time to identify and refresh their paths.

By comparison, diligent protocols often know the whole network and change the routes on a regular basis. This is good for large-sized network but takes enormous memory and computational overhead. In order to tackle this issue, a multihop protocol was developed with both Multipath Optimized Link State Routing (OLSR) and Sequenced Distance Vector (DSDV) / Topology Shift Aware-based Ruting Protocol (TARCS) functions and resources. Multipath distance vector on constructive and ad hoc on demand (AOMDV), i.e. Responsible. At the same time, this hybrid technique will be appropriately opted for but a different hiding place is to examine network traffic and harmful events in order to track sensor nodes in a secured manner. In this case, the routing was carried out in multipath mode that is inevitable.

The initial path request transmissions phases are shown in Table 2. Source sends a Hi packet to identify neighbours using the OLSR method via multi-point relays. The relation codes for the modes of connections and neighbours are defined before the formulation of MPRs. The one and two-hop neighbour sets of algorithms in Table 3 have limited redundant inquiries and replies. The following module also updates a topology table for link-state OLSR by checking the sequence of requests and answers. The first selection process of neighbours is given in Table 4 algorithm which works like monitor nodes. In their presence connected to less redundancy of routing talks the neighbours and routes are listed individually. Source 'S' sends INITREQ (Initial Request) to the next hoppers away from the two-hop random interval, so that the sensor nodes wait for INITRES (Initial Response). The ad hoc sensor network may have multiple sources and destinations.

Table 5 algorithm selects forwarding nodes on different channels with their neighbors and forms CMS.

When OLSR completes the training of the CMS, the timer is off, so that the next tracking technique can be activated by AOMDV. The information of nodes and adjacent OLSRs must be extracted from the Protocol Interface Table at this moment. This helps to create the routing route control that is maintained as a Sandwich Routing Table in AOMDV Routing Table. Table 6 algorithm describes the on-demand monitoring and route maintenance on different channels. A monitor that perforates pattern matching in order to verify the behaviour of a node, traffic nodes patterns and validity of transmitting nodes, is obviously chosen as an algorithm from table 7, and the data is crypted using the channel-

based key sections of Two fish algorithm. In order to rapidly update the report on all nodes, OLSR can resume until the on-demand tracking and routing of AOMDV is halted. With minimum time and redundancy OLSR gets alerts from the Protocol interface page. Periodically and reactively Table 8 algorithm proceeds based on the nature of the nodes and the network conditions. In the next segment, MARS, RC6, Serpent and Two Fish algorithms are channel dependents.

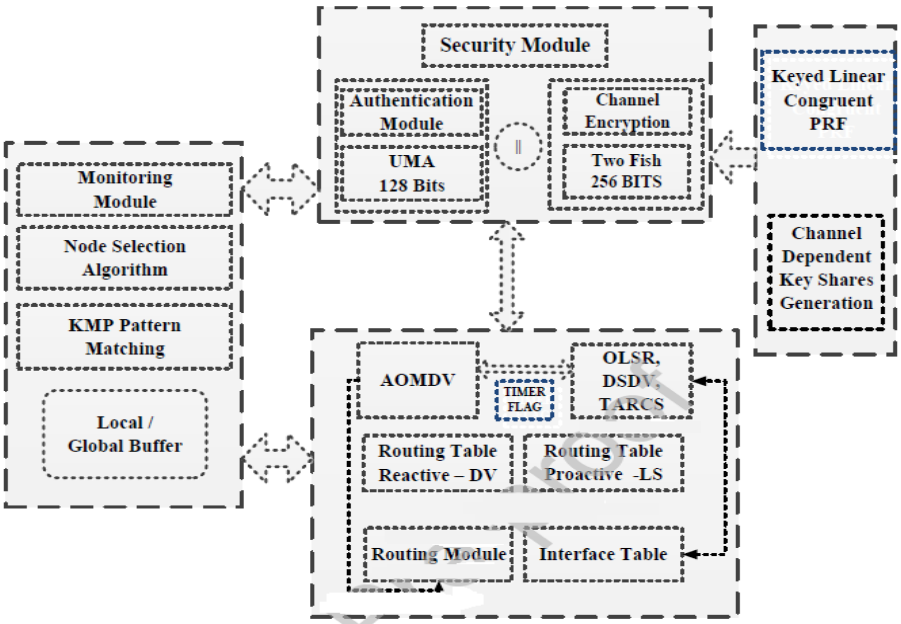

Figure 1: Proposed System Architecture

Table 2: Initial Setup

Hello Message: Initial setup

OLSR HELLO ( )

{

Step1: Source S broadcasts Hello Packets at time T_l;

Step2: One hop Neighbors '$N_1(s)$' receive Hello Packets ;

Step3: N_i of $N_1(s)$ checks Link Type of S; // Bidirectional

if ($LC(0:1)$ && $LC\ (2:4)$ // Check Link Code LC

{ Form $MPR\ (s)$ of Ni ; // Multipoint Relays

Step4: $MPR\ (s)$ retransmits Hello Packets to neighbors ; // Two hop

Step5: Do the same Step 3 for N_{2i} of $N_2(s)$;find seq. num;

Step6: Find the path to destinations D;

Step7: Redo (Periodical) ;

} }

Table 3: Neighbors Identification using MPRs

```
OLSR TC ( )
{
Step1: Where T_i -> T_i + l;  T_i - Current Time ; l -Interval
        If (MPR(s)! = Null)
        {
       // Advertised Neighbor (Seq Number / InfAddr);
        Neighbors identify and Check ANSN && ANIA;
      // Check Sequence Numbers
        If ( ANSN_{i+l}! < ANSN_i )
       { Create TC Table };
        Else
        { Drop TC; }
        }
}
Step2: Redo at T_{i+l}
```

Table 4 Initial Selection

```
OLSR INIT ( )
{
Step 1: If (N_{1i}(s)! = Null && N_{2i}! == Null)
        {
Step 2: If (N_{1i}||N_{2i} not in MPR(s)) // Avoiding Redundancy
        {
        Set broadcast id=1;
        S broadcast INITREQ message to qualified neighbors;
        Wait for Response ;
        }
        Else
        Update N_i Table;
      } }
```

Table 5 Secure Monitoring and Selection for Multiple Channels

```
OLSR MCR ( )
{
Step 1: S receives INITRES from neighbors;
Step 2: N_i = N_i + 1;  N_i(s)-Neighbors;
        where i = {1,2,3,.., hops}
Step 3: If (N_f! = Dest)                    // Neighbor updates
        {
        F_i = F_i + 1;                      // Forwarding Nodes table updates
        }
Step 4: S sends MADV to set of neighbors Ma;
        where M_a = ∑_{i=1}^{3}(N_i − F_i) − U_i
```

Step 5: S computes one-time MAC, $MAC_0 = F(K, M) \parallel P$
Step 6: S waits for MaRES after sending MaREQ;
Step 7: If($MAC_0 == MAC_0^1$)
{
finds, The Eligibility Weight Function (EWF),
$E(f)_{Ma} = \sum_{i=1}^{n}(ES_i \div ET_i) * Bt^{-1} * V^{-1}$
Where, ES_i – Energy spent from sensor node;
ET_i – Total energy assigned in sensor node;
Bt – Data transfer rate (Bit/Sec);
V – Velocity of sensor nodes in mobility;
}
Step 8: If $(E(f)M_a \geq E(f)M_a^R)$ // Compares with reference value;;
{add M_a to List(M); Set $VBit$=1;
$M = M + 1$;// Monitor count;;
Update MTT; If and only if $(T \equiv M \bmod (N/C))$
//builds valid count and topology table;
where$(M \geq 2(N/C))$ // Maintaining at least two monitors for each sensor nodes;;
M – Selected Monitoring nodes; N – Total number of nodes; C – Number of channels;
e – eliminated nodes on setup phase,
and $T\alpha\ Hn$; T – Non –ve integer;
Hn – Number of hops to reach the destination.
} }
Step 9: S Sends $MAS\ (VBit = 1)$ / $MREJ\ (VBit = 0)$ message to neighbors.
Step 10: Update M, Ni, Ds, Ss in PI_Table,
Step 11: Set Timer.$OLSR = OFF$ (t seconds);

Table 6 On-Demand Route Maintenance

Step 1: $If\ (Timer.OLSR = OFF)$
{
$AOMDV\ OP\ START( )$
{

$addList.N_i \leftarrow (PI.T)$; $addList.M, \leftarrow M(PI.T)$;
$addList.D_S \leftarrow D_S(PI.T)$; $addList.Ss \leftarrow Ss(PI.T)$;
Step 2: Mn generates RREQM ; Get RESM;
Step 3: Mn Builds route list (Multi-channels);
Build Concealed Monitor Sets (CMS);
Step 4: M executes PF, (KMP) [ ]
// Pattern Matching
$If\ (EBit! = 1)$ // Check Link Error;;
{
$If\ (PF! = PF1)$
{ // Unsecure node or Channel (ID)
$CID = -1\ (error)$;
$PI.T.RFlag = 1$; Create $PI.T.Report.M$;
// MN-Malicious Node
[where $PI.T.Report.M == KMAC(Mln||CID||T)$];
}
else
{S computes $Cts = MACk_i||Rr\{TFEk_i(MSG_s)\}$;
Here $= 1 \ldots . C$, Rr-Maximum Rounds;
At D, While $(MAC == MAC1)$
{Compute $Pts = Rr\{TFDki(Ct)\}$;}
}
else
{Link error; $(M_n\ (ERRM) \rightarrow S$ through $Next\ Hop)$;
}}
AODV OP WAIT/STOP
(updates $PI.T.RFlag$, $PI.T.Report.M$; Flush out AOMDV RTable)
}
Step 5: Set Timer.$OLSR = ON$; (after t seconds) }

Table 7 Monitoring Report Generation

Step 1: $(If\ Timer.OLSR == ON)$
{
Compute $MPR(s)$; Update $PI.T.Report.M$ in $N(S)$;
$N(s)$ search for route updates;
Continue transmission.
}
Step 2: Repeat the Algorithms.

Table 8 Monitoring Report Updates

Step 1: $(If\ Timer.OLSR == ON)$
{
Compute $MPR(s)$; Update $PI.T.Report.M\ in\ N(S)$;
$N(s)$ search for route updates;
Continue transmission.
}
Step 2: Repeat the Algorithms.

IV RESULTS AND DISCUSSION

This portion includes the specifics of the proposed system's simulation. Algorithms with OTCL (Object Tool Command Language) integration are provided in network simulator Version 2.34. It is a effective method to model ad hoc mobile networks that offer an informative low-level operation to analyze the topology of the network, including sensor nodes, network interfaces, device protocols, and queuing. The routing protocols in this analysis were carefully developed to assess the network's performance and functionality. A systematic approach to studying the pattern of traffic generation and sequence of routing processes is prudently handled in the case of framework analysis containing identification, estimation and isolation. Nevertheless the other ns-versions cannot accommodate or negotiate a traffic structure of end-to-end communication to manage the network load. For that reason, NS-2.34 is favoured where both Multipath Optimized Connection State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols have been implemented with a stable hybrid routing protocol inherited with the properties. This routing protocol manages tactfully to track sensor node operations. The important simulation parameters are listed in table 9. As a MAC layer that sets the propagation range to be 140 m, it uses IEEE 802.11b. With a contact speed ranging from 0 m/s to 5 m/s, every node travels. The contact nodes are grouped due to elevated mobility. The routing protocols, both existing and planned ones, could not, however, be sufficient for a highly complex network. The protocols use a transportation layer protocol, i.e.. 512/10.24 byte Stable Bit Rate User Datagram (UDP) (CBR). The simulation was conducted for 500 seconds in order to evaluate coordination parameters such as monitor intensity and detection ratio. It has a touch node community in the 600 m X 600 m range, which randomly uses malicious nodes to evaluate mobility and data colliding. Most notably, the spatial network area can be set as 200 m X 200 m, 400 m X 400 m, 800 m X 800 m, 1000 m X 1000 m to evaluate the network results. Providing high mobility conditions in a diversified network, a scale of 600 m X 600 m is chosen to measure connectivity metrics such as monitor rate, wormhole attack detection ratio, and IP spoofing attack detection ratio. In addition, it should be remembered that to test the threats, including wormhole and IP spoofing, the malicious behavior is set to be around 15 percent.

Ad-hoc sensors with a total area of 600 m x 600 m are initially installed in various areas. 200 ad-sensor nodes have been developed that roam randomly from one location to another. To locate the set of monitors and other nodes dynamically, this network architecture is taken in the format of a random disc graph with a few edges E and vertices V. Adversaries are often equipped with various capabilities to insert attacks on any connections or nodes in motion (packet dropping, wormhole, IP spoofing).

International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-13 Issue-01 April 2024
https://ijgst.com.2024.v13.i1.pp90-105

Table 9 Details of simulation parameters

Constraints	Values
Network Size	600 m X 600 m
Number of Nodes	200 Nos.
Initial Energy	10 Joules
Simulation Time	100 Seconds
Security Module	HMAC , TF-256 Bits, Key Generation
Routing Protocol	DSDV/OLSR/AOMDV/TARCS/Secure Hybrid Routing
Channel Model	Two Ray Ground Propagation
Data Transmission Mode	Constant Bit Rate (CBR)
Antenna	Omni-Directional
Data Packet Size	512 / 1024 Bytes
Data Transmission Rate	16 Kbps
MAC Protocol	IEEE 802.11b i.e. Distributed Coordination Function (DCF)
Range of Transmission	140 m

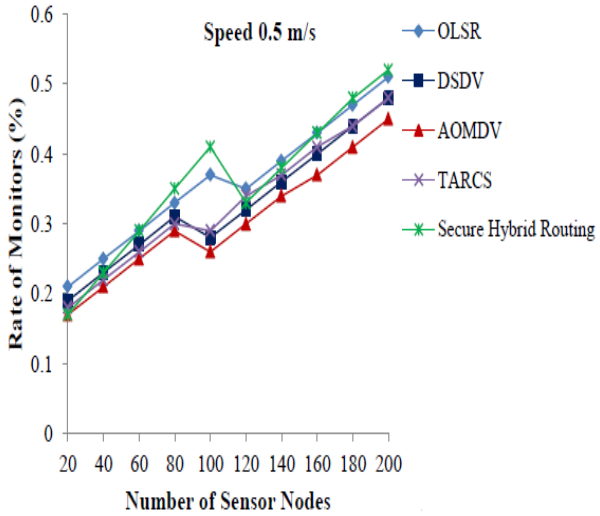

Fig. 2 Number of Sensors versus Rate of Monitor Nodes (Speed 0.5 m/s)

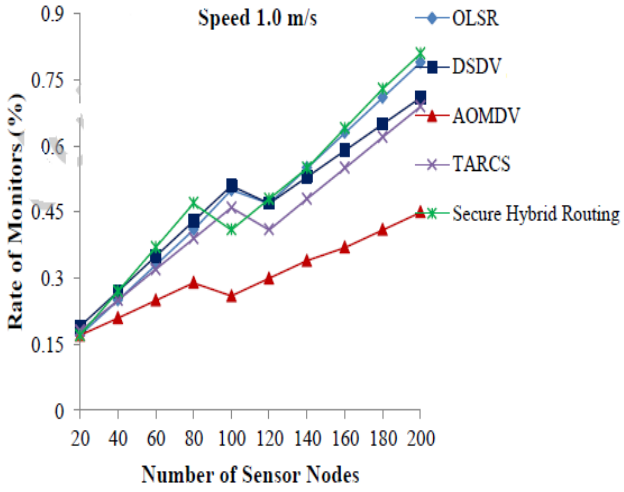

Fig. 3 Number of Sensors versus Rate of Monitor Nodes (Speed 1.0 m/s)

https://ijgst.com.2024.v13.i1.pp90-105

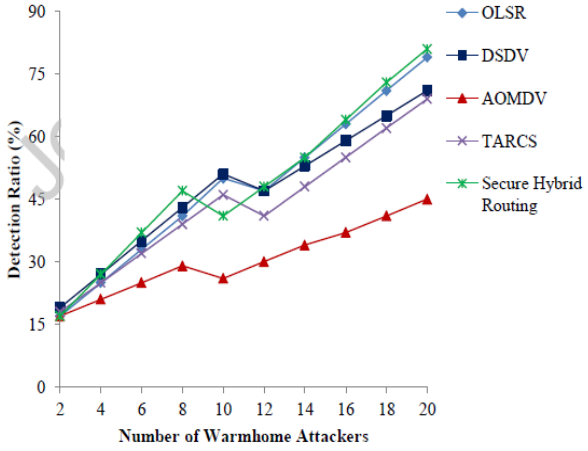

Fig.15 Detection Ratio of Wormhole Attack

Fig.4 Detection Ratio of Wormhole Attack

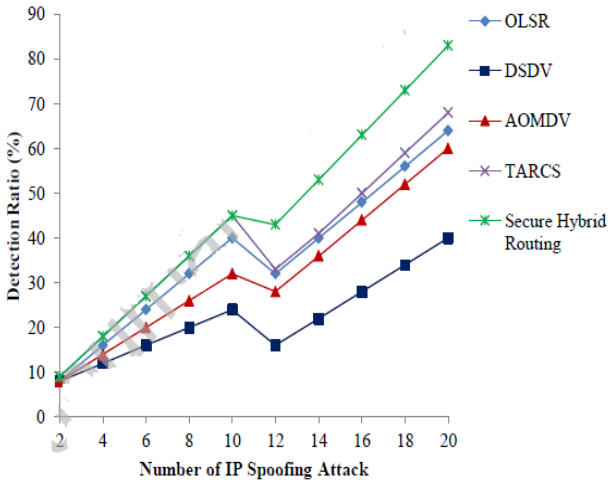

Fig.5 Detection Ratio of IP Spoofing Attack

Both Fig.2 and Fig. 3 gives information of the total number of sensor control nodes and the rate at which the control sensor nodes are chosen against the total number of network nodes available. This shows that the rate of selected monitor nodes, i.e. for safe hybrid routing, remains at 17-52 percent and 50 percent-80 percent in any situation that ensures maximum availability of the routing nodes on multichannel while the nodes move at 0.5 m/s and 1.0 m/s respectively speeds.

In addition, the proposed stable hybrid routing protocol stabilizes the routing system in order to pick a protected node that is trustworthy. The proposed protected routing protocol achieves greater safety performance and node reliability relative to other routing protocols due to less energy usage and a good distribution factor.

The attack detection ratio for wormhole and IP spoofing assaults as seen in Fig 4 and Fig 5. In order to overhear the data transfer on the MAC and routing layer, the attackers attempt to hack the channels or the nodes. The plot provides a sense of protection against increasing attackers from mobile sensors. This displays the effects of the attack detection ratio for multiple attacks on network connections and nodes over the chosen sensor monitor nodes.

In addition, the results of overhead routing during the formation of the network route over aspects of mobility are provided. The established protocols were compared with the proposed safe routing scheme when comparing the analysis performance. This finding shows that, although the network is congested or nodes switch randomly, the initial routing overhead of the proposed solution is peacefully controlled.

Due to optimal security and random power, two-fish have been chosen with H-MAC or for provider multi-channel defence within this network. The primary generation of the node wise random tuples took place at the same time. The suggested solution defines and selects the sensor nodes for routing and monitoring functions that would not allow one sort of node to be accepted in the manner of others.

The data can be routed in the best direction across several canals using authenticated transmitting nodes and a heavily encrypted format. Any additional routing conversations are needed for the initial selection of monitoring nodes and route creation. That needs to be understood

in the rising overhead of routing than most approaches to routing.

However, it decreases steadily once the sensor nodes are chosen with limited delay for routing and tracking for the first time using the OLSR protocol. After the initial selection process, AOMDV keeps the route liveliness continuously through the OLSR cycle expires.

In addition, the optimum or sensor nodes with the least data transmission rate or minimum velocity are taken from the suitable paths for the monitor node selection process. This would in no way significantly damage the overhead of the sensor nodes or the overhead of the network. Compared to MARS, RC6, Serpent, and Twofish, the suggested hybrid routing offers the best protection and randomness in small sensor node processors to understand the significance.

V CONCLUSION

To facilitate protected data transfer, the proposed hybrid routing and monitoring mechanism has been planned and deployed with dynamically chosen sensor monitor nodes in ad hoc sensor networks. A stable protocol for routing and monitoring was suggested with multi-variant tuples that provide scalable protection by symmetrical key methods such as MARS, RC6, Serpent and Twofish. The adversaries in the global sensor network were uncovered and stopped by this suggested tactic.

The Eligibility Weight Feature (EWF) is an authentication and encryption model (ATE) which uses a dynamic symmetrical key to select sensor guard nodes. The suggested hybrid solution uses the node selection algorithm that selects the sensor control node with the aid of the MARS, RC6, Serpent, and Twofish solution to boost with strong security measures. This method helps the ad hoc sensor network to improve the transmission of safe data. The sensor guard nodes are chosen using the Eligibility Weight Feature (EWF) t o reduce the effects of malicious activity to a minimum.

The suggested hybrid secure routing achieves improved tracking and detection ration rates compared to other existing protocols, a detailed simulation reveals. In the future, in order to verify the analysis results, a real-time test bed will be set up to incorporate the hybrid routing and tracking mechanism. In addition, IoT-based WSNs can be used to authenticate the confidentiality of device settings, such as smart cities.

REFERENCES

1. J. Rifkin, “The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism: Book,” Apr. 2014.

2. A. Grau, “The Internet of Secure Things What is Really Needed to Secure the Internet of Things? Icon Labs,” Mar. 2014. [Online]. Available: http://www.iconlabs.com/prod/internetsecurethings-% E2%80%93-what-really-needed-secure-internet-things.
3. U. N. IDC, Intel, “A Guide to the Internetof Things Infographic,” Feb. 2015.Online].Available:https://www.intel.com/ content/www/us/en/internet-of-things/info-graphics/guide-to-iot.html.

4. F. Al-Turjman, H. Zahmatkesh, "An Overview of Security and Privacy in Smart Cities‟ IoT Communications", Wiley Transactions on Emerging Telecommunications Technologies, 2019. DOI. 10.1002/ett.3677.

5. F. Al-Turjman, “Intelligence and Security in Big 5G-oriented IoNT: An Overview”, Elsevier Future Generation

Computer Systems, vol. 102, no. 1, pp. 357-368, 2020.

6. O. Vermesan and P. Friess, "Internet of Things Applications - From Research and Innovation to Market Deployment Book," River Publishers, Jun. 2014. [Online]. Available: http://www.internet-of-thingsresearch.eu/pdf/IERC Cluster Book 2014 Ch.3 SRIA WEB.pdf.

7. I.F. Akyildiz et al., "Wireless sensor networks: A survey", Computer Networks 38 (4) (2002) 393–422.

8. Yun Zhou et al., "Securing Wireless Sensor Networks: A survey", IEEE Communication Surveys, Volume 10, No.3, 2008.

9. S.H. Jokhio et al., "Node capture attack detection and defence in wireless sensor networks, Published in IET Wireless Sensor Systems", 8 August 2011.

10. Abror Abduvaliyev et al., "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013.

11. Yuxin Mao, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", Networked Computing (INC), 6th International Conference, Gyeongju, South Korea 2010.

12. Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, "An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network", Journal of Networks, Vol. 5, Number 3 March 2010.

13. S. Agrawal and J. Agrawal, "Survey on Anomaly Detection using Data Mining Techniques," Procedia Computer Science, vol. 60, pp. 708–713, Jan. 2015. [Online]. Available: http: //www.sciencedirect.com/science/article/ pii/S1877050915023479.

14. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

15. L. Wang and R. Jones, "Big Data Analytics for Network Intrusion Detection: A Survey," International Journal of Networks and Communications, vol. 7, no. 1, pp. 24–31, 2017.

16. P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection," IEEE Communications Surveys Tutorials, pp. 1–1, Jun. 2018.

17. Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the- Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow"s Intelligent Network Traffic Control Systems," IEEE Communications Surveys Tutorials, vol. 19, no. 4, pp. 2432– 2455, 2017.

18. E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey," arXiv:1701.02145 [cs], Jan. 2017, arXiv:

1701.02145. [Online]. Available: http://arxiv.org/abs/1701.02145.

19. Sarkar, S.K.; Basavaraju, T.G.; Puttamadappa, C. Routing Protocols. In Ad Hoc Mobile Wireless Networks-Principles, Protocols, and Applications, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2012; pp. 81–126.

20. Clausen, T.; Jacquet, P. Optimized Link State Routing Protocol (OLSR), RFC 3626 (Experimental). Available online: https://www.ietf.org/rfc/rfc3626.txt.pdf (accessed on 9 October 2018).

21. Perkins, C.E.; Bhagwat, P. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proceedings of the conference on Communications architectures, protocols and applications (SIGCOMM94), London, UK, 31 August–2 September 1994; pp. 234–244.

22. Radhika Ranjan, R. Random Waypoint Mobility, Reference Point Group Mobility. In Handbook of Mobile Ad Hoc Networks for Mobility Models; Springer: Boston, MA, USA, 2011; pp. 637– 670.

23. Fan, B.; Sadagopan, N.; Helmy, A. The Important Framework for Analyzing the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks. Ad Hoc Netw. 2003, 1, 383–403.

24. Hong, J.; Zhang, D. Impact Analysis of Node Motion on the performance of FANET routing protocols. In Proceedings of the 14th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom2018), Chongqing, China, 18–20 September 2018.

25. Sakhaee, E.; Jamalippour, A.; Kato, N. Aeronautical Ad Hoc Networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2006), Las Vegas, NV, USA, 3–6 April 2006; pp. 246–251.

26. Zheng, Y.; Wang, Y.; Li, Z.; Dong, L.; Jiang, Y.; Zhang, H. A Mobility and Load aware OLSR routing protocol for UAV mobile ad-hoc networks. In Proceedings of the 2014 International Conference on Information and Communications Technologies (ICT2014), Nanjing, China, 15– 17 May 2014.

27. Bamis, A.; Boukerche, A.; Chatzigiannakis, I.; Nikoletseas, S. A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks. Comput. Netw. 2008, 52, 130–154.

28. Yu, Y.; Ru, L.; Chi, W.; Liu, Y.; Yu, Q.; Fang, K. Ant colony optimization based polymorphismaware routing algorithm for ad hoc UAV network. Multimed. Tools Appl. 2016, 75, 14451– 14476.

29. Swidana, A.; Abdelghanya, H.; Saifana, R.; Zilic, Z. Mobility and Direction Aware Ad-hoc on Demand Distance Vector Routing Protocol. Procedia Comput. Sci. 2016, 94, 49–56.

30. Khalaf, M.; Al-Dubai, Y.; Min, G. New efficient velocity-aware probabilistic route discovery schemes for high mobility Ad hoc networks. J. Comput. Syst. Sci. 2015, 81, 97–109.

https://ijgst.com.2024.v13.i1.pp90-105

31. Perkins, C.E.; Royer, E.M. Ad-hoc on-demand distance vector routing. In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 25–26 February 1999.

32. Brahmbhatt, S.; Kulshrestha, A.; Singal, G. SSLSM: Signal Strength Based Link Stability Estimation in MANETs. In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks, Jabalpur, India, 12–14 December 2015.

33. Alejandro Proan˜o and LoukasLazos, "Packet Hiding method for Selective Jamming Attacks", IEEE Transactions on Dependable and Secure Computing", Volume 1, January/February 2012.

34. Abderrezak Rachedi and HendBaklouti, "MuDog: Smart Monitoring Mechanism for Wireless Sensor Networks based on IEEE 802.15.4 MAC", IEEE International Conference ICC 2011.
35. Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi, and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure computing, February 2011.
36. Xiao Zhenghong and Chen Zhigang, "A Secure Routing Protocol with Intrusion Detection forClustering Wireless Sensor Networks", International Forum on Information Technology and Applications, 2010.