Analysis and Development of Efficient Wireless Sensor Network

Poonam Sahu[1], Prof. S. R. Yadav[2]

[1]PG Scholar, Mtech(CSE), [2]AP & Head, CSE.

Millennium Institute of Technology and Science, Bhopal

Abstract-In The nodes in WSN are energy constrained since nodes operate with limited battery energy. If some nodes die early due to lack of energy, they cannot communicate with each other. Nodes within an ad hoc network generally rely on batteries (or exhaustive energy sources) for power. Therefore, inordinate consumption of nodes energy should be prevented to enhance working capability of sensors. In fact, node energy consumption should be balanced in order to increase the energy awareness of networks. In this dissertation the proposed security scheme is detect and prevent vampire routing in WSN. We have a tendency to conjointly compare proposed work with normal routing performance and routing performance in case of attacker. We detect vampire attack on the basis of heavy flooding of packets with early depletion of node energy and these packets are consumes the un-necessary energy of other normal nodes because in every action perform by node is consumes limited source of energy. Security is required in WSN because attacker is consumes the useful energy of nodes i.e. necessary for communication in network. The normal performance of WSN is very well known and unusual performance of network is identified by proposed IDS. The comparison of normal and attacker presence is identified the network abnormal conditions. The IDS is also check the status of energy consumption with respect of successful data receiving and routing packets flooding in network. The performance of proposed scheme is gives better routing performance and remove attacker existence in WSN.

Index Terms— Energy, Vampire attack, Routing, Security, Survey, WSN.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of mobile nodes working without any fixed communication infrastructures or base stations to provide connectivity [1, 2]. The nodes are also work with base stations but these nodes are not continuously changing their location. Each node in the WSN acts both as a host and a router. If two nodes are not within the transmission range of each other, other nodes are needed to serve as intermediate routers for the communication between the two nodes. The hosts are free to move around randomly, and hence the network topology may change dynamically over time. One of the first WSNs was designed and developed in the middle of the 70s by the military and defense industries. WSNs were also used during the Vietnam War in order to support the detection of enemies in remote jungle areas. However, their implementation had several drawbacks. It includes the large size of the sensors, the energy they consume and the limited network capability. Due to absence of administrative control network security is the major criteria. The attacker or malicious node like Vampire attack [2] has consumed limited energy resource [1] by that the life time of network is affected. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy constrained nature of such networks [2]. For example, flooding is a technique in which a given node broadcasts data and control packets that it has received to the rest of the nodes in the network. This process repeats until the destination node is reached. Note that this technique does not take into account the energy constraint imposed by WSNs. This information is usually created accessible to the user through one or more intermediate nodes [3,4] WSN Challenges and Routing Issues. The design of routing protocols for WSN is difficult owing to many network constraints. WSN suffer from the restrictions of many network resources, as an example, energy, bandwidth, central process unit, and storage [5, 6]. The planning challenges in networks involve the subsequent main aspects [3, 5, 6].

II. ROUTING PROTOCOLS IN WSN

Routing in wireless sensor network (WSN) differs from conformist routing in fixed networks in various ways. The sensor node done routing without any fixed infrastructure, wireless links are unreliable, sensor nodes possibly will fail, and routing protocols have to congregate stringent resources requirements [8, 9, 10]. Routing paths can be established in one of three ways, namely proactive, reactive or hybrid..

A. Proactive (table-driven) Routing Protocol

The proactive routing protocol is the table driven protocol to managing the table of route information in network. The proactive routing protocol are showing the better performance in fixed or stationary network because the routing table updation is not possible their but in dynamic sensor network the routing information is changes by that the overhead in network is more. The most well-known types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol.

B. Reactive (on-demand) Routing Protocol

The reactive routing protocols re maintaining the connection in a On demand manner means if required then established connection. The routing protocol are flooded the route request and if the destination found data delivery is started but after the completion of routing procedure including data sending route information is completely destroyed in from nodes that has participating in routing. The Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol is the example of that kind of routing.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [11].

III. LITERATURE SURVEY

In WSN energy and wireless interference while heavily rely on selecting most trusted neighbors and if the limited resource is consume then the attacker possibility is high. Some previous researches are as follows:-

This paper [12] has only identified that the Vampire attacks can be easily executed using even a single malicious intruder, who sends simply protocol complaint message, these attacks are thus destructing and very hard to detect. In the worst condition, particular single attacker has the ability to extend the energy usage of the network by a factor of O(N), where N is the quantity of nodes in the network. A new proof-of-concept protocol is a method discussed to mitigate these kinds of attacks. This protocol limits the damage caused at the time of packet forwarding done by Vampires. To diminish the Vampire attacks using PLGP-a (parno ,luk, gausted and perrig wih attstations) which identifies malicious attack, certain approaches have also been discussed. PLGP stands for a clean-slate secure sensor network routing protocol by parno ,luk, gausted and perrig.

Vidya.M [13] In this paper a innovative approach for routing protocols, affect from attack even those devised to be protected which is short of protection from these attacks, which we call energy debilitating attacks, which enduringly disable networks by quickly draining nodes battery power. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. They also saw how to overcome these attacks by increasing the energy of the node in the network.

In this paper [14], a Trust and Energy aware Routing Protocol (TERP) has been specifically designed to address the limitations of existing trust based routing protocols. Keeping resource-constrained characteristic of WSN in mind, the design of TERP is centered on trustworthiness and energy efficiency. TERP is capable of dynamically detecting and isolating misbehaving nodes during trust evaluation phase while energy awareness feature is incorporated in route setup phase of routing protocol which helps in better load balancing among trusted nodes. The TERP protocol has been designed to integrate trust based routing but additionally includes mechanisms which ensure that end-to-end routes are selected while keeping in view the current energy levels of the intermediate nodes.

Ambili M.A [15] In this we define that a Network survivability is the ability of a network keeping connected under failures and attacks, which is the primarily significant issue in the designing and performance of WSN. The research is focus on the technique in which the attack can be overcome in the best possible manner. The proposed system describes some methods and alternative routing protocols solution that helps to detect and eliminate vampire attack and thus make the network live. An energy constraint intrusion detection scheme is introduced along with clean state secure routing protocol.

C. Karlof, N. Sastry, D. Wagner, TinySec [16] uses link-layer security architecture to guarantee message authenticity, integrity, and confidentiality. Message authenticity is the ability to detect false messages and reject them. Similar to message authenticity is message integrity, the detection of a tampered message. The TinySec gives integrity and message authenticity by including a message authentication code (MAC) with each packet. The MAC is a cryptographically secure checksum of a message. The MAC is computed using a share secret key between the sender and the receiver. The sender computes the MAC of a packet using its secret key. The packet and the MAC are sent to the receiver. The receiver sharing the same secret key re-computes the MAC value of the message and compares it against the MAC received. If the keys are the same then the packet is received by receiver else it is dropped in network. If an malicious node/s modify the message during transit then sender would not be able to re-compute the MAC value. Hence, the receiver will reject the message. Message confidentiality keeps information safe from unauthorized members. Now in that type of condition, the encryption mechanism should achieve reliable security. Reliable security implies that adversaries cannot learn any property of the message even if they have obtained the message.

In this paper [17], a novel trust routing scheme is proposed. Multi-agents collect multi-factors information and cooperate to decide the trust route. Trust computing maybe needs the support of hardware architecture and embedded processor technology. Trust and reputation have been recently suggested as an effective security mechanism for open environments such as sensor network. The performance and security of sensor networks depend on trust in distributed nodes. To enhance security in sensor networks, it is important to evaluate trustworthy degree of nodes. To a single node, it's difficult to know whether to trust the other nodes with its own information and knowledge, especial in routing discovery step, selecting a trust path is important to build a security WSN network. Traditional security methods which provide confidentiality, authentication, and availability are not efficient to sensor network because of the special network application scenarios. Traditional cryptographic technology is difficult to process active attacks. Trust is the degree of belief about the future behavior of other entities, which is based on the past experience of the nodes. To sensor network, if WSN nodes want to communicate or exchange key data, it is necessary to establish trust relationship between nodes to ensure the reliable data exchange. Trust is related to many factors, such as hop count, node behaviour, and node's residual energy.

In this paper [18] proposed new Reputation-based Framework for Sensor Networks (RFSN). This is the reputation and trust-based model designed and developed exclusively for sensor networks, which using watchdog mechanism to build trust rating. New trust scheme is necessary to the special characteristics of the sensor network. Each sensor node develops a reputation for each other node by making direct observations about the other neighbor nodes. This reputation is used to help a node evaluate the trustworthiness of other sensor nodes and make decisions within the network. But the watchdog cannot record all the behavior due to its own fault or network error, so there is some uncertainty events in the trust system. Mutual entity authentication plays an important role in securing wireless sensor networks.

IV. PROPOSED SCHEME AGAINST VAMPIRE ATTACK

The attacker nodes are communicated with other nodes at the time of routing procedure and it is not unnecessary flooded infected packets in network. The attacker behavior is identified through IDS by capturing the unwanted packets and also not participating in routing procedure as like other sensor nodes. The energy consumption is also uncontrolled and according to that packets are receiving is not satisfactory.

The whole procedure of Vampire attacker detection and prevention through IDS is mentioned in proposed algorithm.

A. Proposed Algorithm to Detect and Prevent Network from Attack

```
Wi: Wireless Sensor Nodes  // i =1, 2, 3.............n for all where i exist

Si: Represents sender nodes // Si ϵ Wi

Di: Number of Receiver nodes // Ri ϵ Wi

Ii: Intermediate Nodes // Ii ϵ Wi

Routing protocol = AODV // Ad hoc On Demand Distance Vector

Ei: Energy of Nodes // Consider energy initial level randomly

Vi: Vampire Attacker Nodes

IDS: IDS or Prevention node

Sender Si broadcast (RREP, Ei, AODV)   // RREQ stands for Route Request Packets

If (Ei >0 && Route from Si   Receives RREP && hop-count > 1)  //RREP stands for Route Reply
  Packets//

{
   If (Next Node == Di) // hop count is 1 and destination is directly available
         {
          Reply RREP of  RREQ ;
          Confirm connection from Si
           Si sends data packets to Destination Di;
            }
       Else
       {
     Intermediate node/s Ii exists in route;
     RREQ forwarded receives RREP by Ii to I i+1, I i+2....... In till destination not found;
          Di reply to Si for data sending and Si sends data to Di;
         }
        If (Intermediate node Ii status  = = Abnormal) // abnormal is stands for heavy flooding and early energy depletion confirm by IDS//
            {
            If (abnormal == Additional Flooding || Energy Depletion)
            {
            IDS node is Perform actions against Abnormal Behavior;
```

```
                Packets are other than RREQ, RREP and Data;
Identify their abnormality;
                Gain energy of sender and other nodes;
                }
                }
Else if (Intermediate node Ii status = = normal) // normal stands for no malicious actions are performances in network//
                {
                No any attack
                Send data through that path
                }
                }
IDS capture all nodes Ii information, Vi abnormal status, Node ID, Energy information of Abnormal Node)
        {
        If (IDS receives malicious information through Vi neighbour)
        {
                Directly communicate to attacker for update unfaithful status;
                If (Status of Vi != Update)
        {
Broadcast Vi malicious activity to all alive nodes
Block the Vi attacker node // block through off their communication
        }
        Else if (Status of Vi = = Normal
        {
        Path is future established
        Indentified attacker node by IDS
        }
        }
        }
Stop
```

The attacker is the intermediate nodes which is not accept packets it is only flooded. These packets are not utilized for any purpose in network. The quantity of these packet are large in quantity and these packets gradually busy all intermediate nodes or receiver nodes to busy for receiving packets of attacker in WSN. All the sensor nodes are only work for malicious nodes and malicious nodes are enhancing the quantity of flooding according to time instance.

V. SIMULATION PARAMETERS

We analyze the time when each node die due to lack of remaining battery (i.e., expiration time of nodes) as well as the lifetime of connection which captures the effects of disconnections due to lack of possible routes (i.e., expiration time of connections). The simulation parameters are considered for simulation is mentioned in table 1.

Table 1 Simulation Parameters for Case Study.

Simulator Used	NS-2.31
Number of nodes	50
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100
Traffic type	CBR (3pkts/s)
Packet size	512 bytes
Number of traffic connections	TCP / UDP
Node movement at maximum Speed (m/s)	random
Transmission range	250m
Threshold value	10 joule
Transmit power	1.5 joule
Receiving power	1.0joule
Idle power	.17 joule
Sleeping power	.047 joule

VI. RESULTS AND DISCUSSION

The results description in detail is discuss in this section. Here the performance of proposed IDS scheme is compare with previous EAODV protocol in WSN.

A. Vampire Attacker Loss Analysis

Vampire attack consumes the energy of normal nodes and decreases the performance of the network and while more node energy is utilized for fewer packets receiving then network split in number of sub network and increase the network overhead. The number of nodes in network is flooded large amount of data packets and these packets are consuming network limited energy resource. In this graph performance of only attacker loss is measured and identified that the up to end of simulation time 100 seconds about 25% are drop due to presence of attacker but after applying IPS scheme not a single packet is drop due to attacker infection in sensor network.

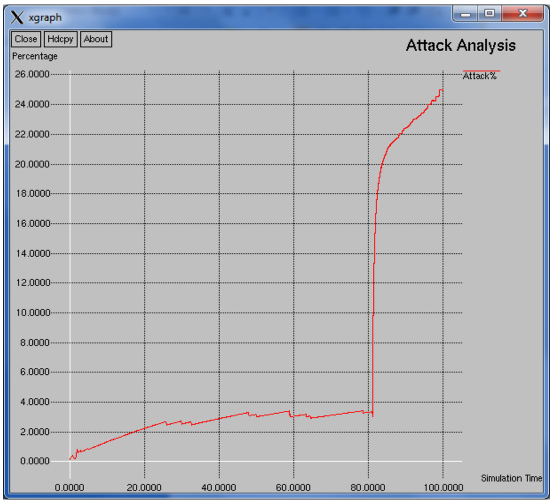

Fig.1 Attacker Loss Analysis

B. Attacker nodes Packets flooding and Percentage of infection

In the Sensor Network many nodes are having malicious behaviour that flooding number of packets. But due to continuously activation of some nodes another malicious nodes are not fully participating for injecting infection in WSN. In table 1 the attacker nodes packets flooding with loss percentage are mentioned. After applying IPS these attacker infection is totally removes from sensor network.

Table 2 Attacker Nodes Analysis

Vampire Node	Packet Capture	Percentage of Infection
12	93	0.01
17	112	0.01
26	226740	29.03
34	484	0.06
36	15012	1.92

C. Packet Delivery Ratio Analysis

The Packer Delivery Ratio (PDR) is measure for evaluate the percentage of successful data receiving with respect to sending in sensor network. The network is completely dynamic and in this network the vampire attacker presence is incessantly humiliate the sensor network performance. In presence of Vampire attacker the lowest performance is about 5% and highest is about 60% at the starting time of simulation. The packets successful percentage is enhanced after applying proposed IPS scheme and the successful packets receiving is reaches up to 90% up to end of simulation time in WSN.

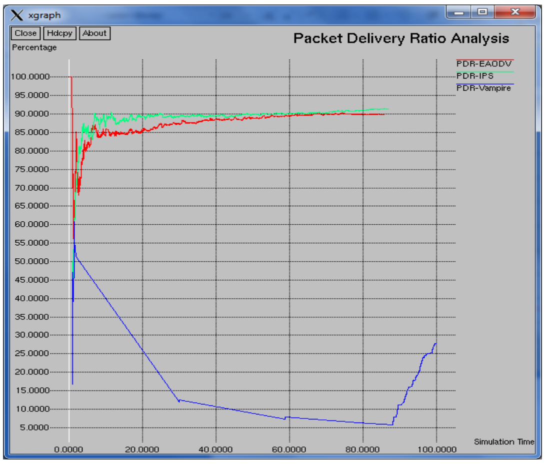

Fig .2 PDR Analysis

D. Routing Overhead Analysis

The routing packets flooding are generated through to find the destination. The packets flooding is scattering in network up to destination is not found. The intermediate nodes are more in between sender and receiver then the possibility of flooded is also more. In this analysis the packets flooding analysis is measured in normal routing scenario, in presence of attack and in presence of IPS security scheme in WSN. Here due to attacker flooding the quantity of flooding packets are beyond the estimation and because of that the particular attacker recognized by IPS security system and then minimizes the overhead in WSN.

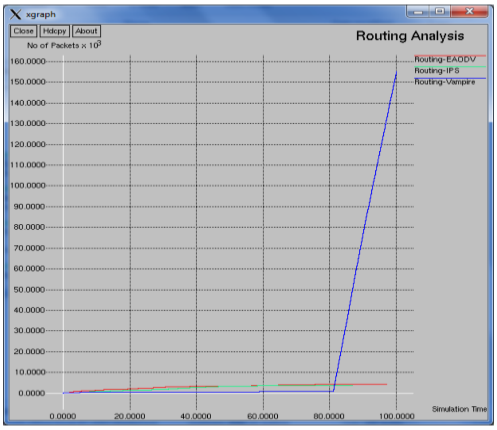

Fig. 3 Overhead Analysis

E. Throughput Performance Analysis

The throughput performance of network is gives the information about the number of data packets receiving at destination in unit interval of time. The throughput is also evaluated in bits/seconds. In this graph the performance of proposed IPS is again gives the better results that showing the improving in routing performance. In this graph the maximum throughput in presence of IPS is about 1450 packets/seconds but in presence of Vampire attack throughput performance is almost count negligible. The performance of IPS is better than normal EAODV routing because in IPS the same route establishment conditions are change and changeable condition are in favour of security scheme in WSN.

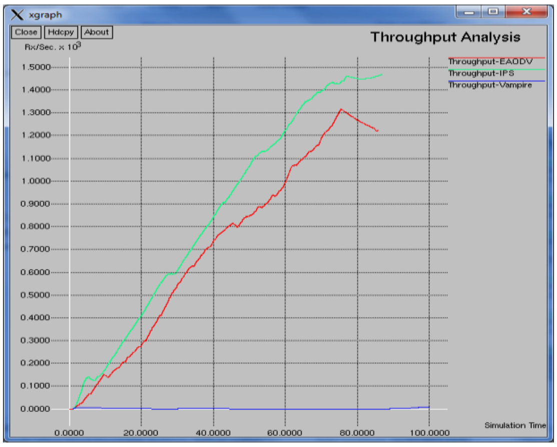

Fig.4 Throughput Analysis

VII. CONCLUSION & FUTURE WORK

The Vampire attacker is flooding the huge amount of packets in network and every node in network is capture and forwards these packets to next neighbor. The packets sending and receiving is consumes the lot of energy. The proposed security scheme is detect the attacker on the basis of packets flooding with higher amount of energy consumption in packet receiving. The proposed IDS algorithm is detect attacker and identified the routing misbehavior in network. The working of nodes is battery power or energy dependent having limited lifetime and this energy is consumed by attacker unnecessary in network. In attacker presence the packet receiving in network is minimizes but the energy consumption according to packet receiving is more. The flooding of packets is shows the abnormal behavior of network conditions. This proposed work against Vampire attack is examined and relevant methodology for improving security and performance of network also distinguishing and removing suspicious node from the network. The performance of same network scenario is measure in normal routing, routing in presence of Vampire attack and IDS apply on Vampire attack. The performance of proposed scheme is provides the better results and this scheme is also provides the safe and sound message delivery in presence of disable attacker. The rest of network performance in term of throughput, packet receiving is improve and delay and overhead is reduces in dynamic WSN.

We will detect vampire attack on the basis of heavy flooding of packets but at this time instant we identified attacker rapidly because we already know their malicious behavior. We also apply one more sinkhole attack in network and measure combined malicious performance and also implement new IDS scheme for that combined attacker malicious effect in WSN.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks, Elsevier, pp. 2292–2330, 2008.

[2] A.Vincy, V.Uma Devi, "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014

[3] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[4] S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[5] Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Communications Magazine, vol 11, no. 6, pp. 6-28, Dec. 2004.

[6] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices", IEEE Personal Communication Magazine, vol. 7, no. 5, pp. 28-34, Oct. 2000.

[8] Clement Ogugua Asogwa, Xiaoming Zhang, Degui Xiao, Ahmed Hamed, "Experimental Analysis of AODV, DSR and DSDV Protocols Based on Wireless Body Area Network" Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg,Volume 312, pp 183-191, 2012.

[9] Faleh Rabeb, Nasri Nejah, Kachouri Abdennaceur,Samet Mounir, "An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network" IEEE, International Conference on Education and e-Learning Innovations, 2012.

[10] Nasrin Hakim Mithila, "Performance analysis of DSDV, AODV and DSR in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 2, Issue 4, pp.395-404, April 2013.

[11] Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM/IEEE Transactions on Networking, Vol.9, No.4, pp.427-438, August 2001

[12] Lina R.Deshmukh, Prof. A. D. Potgantwar, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", IEEE International Conference on Advance Computing (IACC), pp. 61 - 66, 12-13 June 2015.

[13] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network", IEEE Sensors Journal, Vol. 15, No. 12, December 2015.

[14] Ambili M.A, Biju Balakrishnan, ''Vampitr Attack: Detection and Elimination in WSN", IJSR Vol- 3 April 2014.

[15] Vidya.M, Reshmi.S, ''Alleviating Energy Depletion Attacks in Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[16] C. Karlof, N. Sastry, D. Wagner, TinySec, "A link Layer Security Architecture for Wireless Sensor Networks", in Proceedings of the Sensys'04, Baltimore, MD, 2004.

[17] Chen Hongsong, Han Zhi, Fu Zhongchuan, "Quantitative Trustworthy Evaluation Scheme For Trust Routing Scheme in Wireless Sensor Networks", IEEE Trustcom/BigDataSE/ISPA, pp1273-1278, 2015.

[18] S. Ganeriwal and M. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks", In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN), pp. 66-77, 2004.