ACTIVE TRUST IN WIRELESS SENSOR NETWORKS: LONG-DURABLE ROUTING

Dr.K.C.Ravi Kumar,SURABI PARIDA,Department of Computer Science & Engineering,Raajdhanni Engineering College

Abstract—

Wireless sensor networks (WSNs) are increasingly being used in critical security applications. Because of their inherent resource constraints, they are vulnerable to various security attacks, including a blackhole attack, which has a significant impact on data collection. To address this challenge, ActiveTrust, an active detection-based security and trust routing scheme, is proposed for WSNs. The most significant innovation of ActiveTrust is that it avoids black holes by actively creating a number of detection routes to quickly detect and obtain nodal trust, thereby improving data route security. More importantly, the ActiveTrust scheme provides for the generation and distribution of detection routes, which can fully utilise the energy in non-hotspots to create as many detection routes as required to achieve the desired security and energy efficiency. Comprehensive theoretical analysis as well as experimental results indicate that the performance of the Active Trust scheme is better than that of previous studies. Active Trust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime.
Index Terms—black hole attack, network lifetime, security, trust, wireless sensor networks

I. INTRODUCTION

WIRELESS Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains [1-5]. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks [6-8]. A black hole attack (BLA) is one of the most typical attacks [9] and works as follows. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions [10-15]. Therefore, how to detect and avoid BLA is of great significance for security in WSNs.

There is much research on black hole attacks [9, 16-19]. Such studies mainly focus on the strategy of avoiding black holes [17, 18, 19]. Another approach does not require black hole information in advance. In this approach, the packet is divided into *M* shares, which are sent to the sink via different routes(multi-path),but the packet can be resumed with *T*shares (*T*<=*M*). However, a deficiency is that the sink may receive more than the required *T* shares, thus leading to high energy consumption; such research can be seen in [9, 16]. Another preferred strategy that can improve route success probability is the trust route strategy. There is much related research, such as [20, 21, 22, 23, 24]. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability [22,23].

However, the current trust-based route strategies face some challenging issues [24]. (1) The core of a trust route lies in obtaining trust.However, obtaining the trust of a node is very difficult, and how it can be done is still unclear. (2) Energy efficiency. Because energy is very limited in WSNs, in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the network lifetime. (3) Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue. Thus, there are still issues worthy of further study. Security and trust routing through an active detection route protocol is proposed in this paper. The main innovations are as follows.

(1) The Active Trust scheme is thefirstroutingschemethat uses active detection routing to addressBLA.

The most significant difference between ActiveTrust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will

attack these routes and, in so doing, beexposed.Inthisway,theattacker'sbehaviorandlocation,as well as nodal trust, can be obtained and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism inWSNs.

(2) The ActiveTrust route protocol has better energy efficiency.

Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. However, we find it possible after carefully analyzing the energy consumption in WSNs. Research has noted that there is still up to 90% residue energy in WSNs when the network has died due to the "energy hole" phenomenon. Therefore, the ActiveTrust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots (to improve network lifetime). Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security. According to theoretical analysis and experimental results, the energy efficiency of the ActiveTrust scheme is improved more than 2 timescomparedtopreviousroutingschemes,includingshortest routing, multi-pathrouting.

(3) The ActiveTrust scheme has better security performance.Comparedwithpreviousresearch,nodaltrustcan be obtained in ActiveTrust. The route is created by the followingprinciple.First,choosenodeswithhightrusttoavoid potential attack, and then route along a successful detection route.Throughtheaboveapproach,thenetworksecuritycanbe improved.

(4) Through our extensive theoretical analysis and simulation study, the ActiveTrust routing scheme proposed in this paper can improve the success routing probability by 1.5 timesto6timesandtheenergyefficiencybymorethan2times compared with that of previousresearches.

The rest of this paper is organized as follows. In Section 2, the related work is reviewed. The system model and problem statement are described in Section 3. In Section 4, the novel ActiveTrust scheme is presented. Security and performance analysesareprovidedinSection5.Section6istheanalysisand comparison of experimental results. We conclude in Section7.

II. RELATEDWORK

Single-pathroutingisasimpleroutingprotocol[12]butis easily blocked by the attacker. Therefore, the most natural approach is via multi-path routing to the sink. Even if there is an attack in some route, the data can still safely reach the sink [9]. Multi-path routing protocols can be classified into two classesdependingonwhetherthedatapacketisdivided.Oneis multi-path routing without share division. The other is multi-pathroutingwithsharedivision,i.e.,thepacketisdivided into shares, and different shares reach the destination via different routes[9].

(1) Non-share-based multi-path routing. There are different multi-path route construction methods. Ref. [25] proposes a multi dataflow topologies (MDT) approach toresist the selective forwarding attack. In the MDT approach, the network is divided into two dataflow topologies. Even if one topology has a malicious node, the sink can still obtain packets from the othertopology.

In such protocols, the deficiency is that if the packet is routed via n routes simultaneously, the energy consumption will be n times that of a single path route, which will seriously affect the network lifetime; similar research can be seen in multi-path DSR [25], the AOMDV [18] and AODMV [26].

(2) Share-based multi-path routing protocols. The SPREAD algorithm in [27] is a typical share-based multi-path routingprotocol.ThebasicideaoftheSPREADalgorithmisto transformasecretmessageintomultipleshares,whichiscalled a(T,M)thresholdsecretsharingscheme[28].The$M$sharesare delivered by multiple independent paths to the sink such that, even if a small number of shares are dropped, the secret message as a whole can still be recovered [9, 16, 28]. The advantage of this algorithm is that through multi-path routing, each path routes only one share, and the attacker must capture at least T shares to restore nodal information, which increases the attack difficulty [9]. Thus, the privacy and security can be improved. In the above research, the multi-path routing algorithms are deterministic such that the set of route paths is predefined under the same network topology [9]. This weakness opens the door for various attacks if the routing algorithm is obtained

by the adversary[9].

For the weakness mentioned above, Ref. [29] proposed four random propagation strategies: random propagation(PRP), directed random propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree assisted random propagation (MTRP). The general strategy is as follows. First, divide the message into *M* shares, and the route path of each shareisnotpredetermined.Thus,eveniftheadversaryacquires the routing algorithm, it is difficult to launch a pinpointed node-compromise or jamming attack. Because it is difficult to capture more than *T* shares, the security is also improved. In multi-to-one data collection WSNs, we argue that for classic "slicing and assembling" or multi-path routing techniques, sliced shares will merge in the same path with high probability, and this path can be easily attacked by black holes. Thus, in [16], a Security- and Energy-efficient Disjoint Route (SEDR) scheme is proposed to route sliced shares to the sink with randomized disjoint multipath routes by utilizing the available surplus energy of sensor nodes. The authors demonstrate that the security is maximized without reducing the lifetime in the SEDRprotocol.

Another method to avoid attack and improve route success probabilityistrustrouting.Trustmanagement[20]isbecoming a new driving force for solving challenges in ad hoc networks [21], peer-to-peer networks [22], and WSNs [23,24].

Zhan et al proposed a trust-aware routing framework protocol (TARF), using trust and energy cost for route decisions, to prevent malicious nodes from misleadingnetwork traffic[30].Ref.[31]proposestheSec-CBSNalgorithm,which develops different trust calculation methods based on nodal roles. Ref. [32] develops an attack-resistant and lightweight trust management protocol named ReTrust, which can resist attacks through a trust management approach for medical sensor networks (MSNs). Ref. [33] presents a proposal named TRIP, which aims to quickly and accurately identify malicious orselfishnodesspreadingfalseinformationinvehicularadhoc networks (VANETs). Ref. [34] also proposes a resilient trust model, SensorTrust, for hierarchical WSNs. Ref. [24] introduces the concept of attribute similarity in finding potentially friendly nodes amongstrangers.

Although there is much research on black node attack avoidance,thereisstillmuchthatisworthyoffurtherstudy.(1) The current black hole avoidance strategies mostly affect network lifetime. (2) The current black hole avoidance strategies are mostly passive acting systems, which affects system performance. (3) The trust route mechanism has high costs and is difficult to obtain trust, so the guiding significance is limited [35, 36].

III. THE SYSTEM MODEL AND PROBLEMSTATEMENT

The SystemModel

Network model

(a) We consider a wireless sensor network consisting of sensor nodes that are uniformly and randomly scattered in a circularnetwork;thenetworkradiusis*R*,withnodaldensity

□, and nodes do not move after being deployed [4, 9]. Upon detectionofanevent,asensornodewillgeneratemessages,

and those messages must be sent to the sink node [4, 13].

(b) We consider that link-level security has been established through a common cryptography-based protocol.

Problem Statement

(1) Network lifetime maximization. Network lifetimecan be defined as the first node die time in the network [4, 9, 16]. For E_i as the energy consumption for node i , the lifetime maximization can be expressed as thefollowing:

$$\max(T) \square \min\max(E_i) \quad (3)$$

(2) The data collection has better security performance and strong capability against black holeattacks.

The main goal of our scheme is to ensure that the nodal

datasafelyreachthesinkandarenotblockedbytheblackhole. Thus, the scheme design goal is to maximize the ratio of packets successfully reaching the sink. Consider that the number of packets that are required to reach the sink is □and thatthenumberofpacketsthatultimatelysucceedinreaching
the sink is m ; the success ratio is

$q \square m \square$ (4)

Our goal is to maximize the success ratio, that is, $\max(q)$.

Insummary,theoptimizationgoalofthispaperisthefollowing equation:

$\square \max(T) \square \min \max(E)$

Thus,weconsideralinkkeytobesafeunlesstheadversary $\square 0 \square i \square n$ ^{i}(5)

physically compromises either side of the link [9, 16].

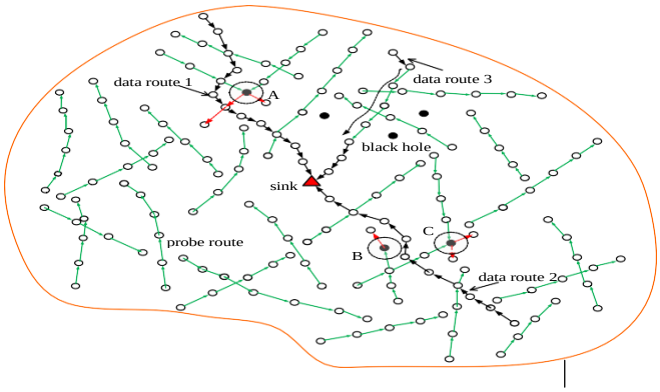
(2) The adversaries model

We consider that black holes are formed by the compromised nodes and will unselectively discard all packets passed by to prevent data from being sent to the sink [9, 16]. Theadversaryhastheabilitytocompromisesomeofthenodes. However, we consider the adversary to be unable to compromise the sink and its neighboring nodes [9,16].

B. Energy Consumption Model and RelatedDefinitions

According to the typical energy consumption model [4,9, 16], Eq. (1) represents energy consumption for transmitting, and Eq. (2) represents energy consumption forreceiving.

E_{elec} represents the transmitting circuit loss. Both the free space (d^2 power loss) and the multi-path fading (d^4 power loss) channel models are used in the model depending on the



$\square \square \max(q) | q \square m \square$

IV. ACTIVE TRUST SCHEMEDESIGN

A. Overview of the ProposedScheme

An overview of the ActiveTrust scheme, which is composed of an active detection routing protocol and data routing protocol, is shown in Fig. 1.

distance between the transmitter and receiver. $\square_{fs}$and$\square_{amp}$
aretherespectiveenergyrequiredbypoweramplificationinthe two models. The energy consumption for receiving an l -bit packetisshowninEq.(2).Theaboveparametersettingsare
shown in Table 1, as adopted from [4, 9, 16].

$\square \square E_{member} \quad \square lE_{elec} \quad \square l \square d^2 \quad if d \square d$

$\square$

$E_0 \quad \square lE \quad \square l \square d^4 if \ d \square d$ (1)

Fig. 1: Illustration of the ActiveTrust scheme

(1) Active detection routing protocol: A detection route referstoaroutewithoutdatapacketswhosegoalistoconvince

□□*member elec amp*

$E_R(l) = lE_{elec}0$
(2)(2)

Parameter	Value
Threshold distance (d_0) (m)	87
Sensing range r_s(m)	15
E_{elec}(nJ/bit)	50
e_{fs}(pJ/bit/m^2)	10
e_{amp}(pJ/bit/m^4)	0.0013
Initial energy (J)	0.5

the adversary to launch an attack so the system can identifytheattackbehaviorandthenmarktheblackholelocation.Thus,the

Table 1 network parameters

system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it caneffectivelyguidethedatarouteinchoosingnodeswithhigh trusttoavoidblackholes.Theactivedetectionroutingprotocol is shown via the green arrow in Fig. 1. In this scheme, the source node randomly selects an undetected neighbor node to createanactivedetectionroute.Consideringthatthelongest detectionroutelengthis□,thedetectionroutedecreasesits

length by 1 for every hop until the length is decreased to 0,and then the detection routeends.

(2) Data routing protocol. The data routing refers to the processofnodaldataroutingtothesink.Theroutingprotocolis similar to common routing protocols in WSNs [3, 7, 8]; the difference is that the route will select a node with high trustfor the next hop to avoid black holes and thus improve the success ratio of reaching thesink.

ThedataroutingisshownviatheblackarrowinFig.1.The routing protocol can adopt an existing routing protocol [7, 12], and we take the shortest route protocol as an example. Node *a* in the route will choose the neighbor that is nearer the sink and has high trust as the next hop. If there is not a node among all neighbors nearer the sink that has trust above the default threshold, it will report to the upper node that there is no path from *a* to the sink. The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sinkor there is conclusively no path to thesink.

B. Active Detection RoutingProtocol

Table 2: Pseudo-code of Algorithm 1 for the active detection routing protocol

Algorithm 1: Active Detection Routing Protocol

1: Initialization
2: **For** each neighbor node A_n Do
3: LetA$_n$.accesTime=Current_time
4: **End** for
5: **For** each node that generates a detection packet, such as node A, Do

head	type	source	□	□	id

Fig. 2: The structure of packets of detection routes

The source node selects an undetected node to launch the detectionroute.Oncethedetectionpacketisreceivedbynodes, themaximumroutelength□isdecreasedby1.Afterthat,if □is0,generateafeedbackpacketandlaunchafeedbackroute to the source, and then restore □to the initial value. If □is not 0, then continue to select the next hop in the same way; otherwise, end the route. The structure of a feedback packet is shown in Fig. 3, and it is also composed of 6 parts: (a) packet head; (b) packet type; (c) ID of the source node; (d)destination node; (e) ID of the detection packet; and (f) ID of thepacket.

head	type	source	Destination	S-id	id

Fig. 3: The structure of feedback packets of a detection route

The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source, and the following is the algorithm for the detection route protocol.

C. Calculation of NodalTrust

During data routing and detection routing, every node will performanodaltrustcalculationtoaidinblackholeavoidance. When node A performs a detection route for node B at time t_i , if the detection data are successfully routed, consider the trust of node A to B to be $\square^B(t$) ; otherwise, consider the trust tobe $\square^B(t)$. Considering that A has w interactions with B during t, the detection value order by time is as follows:

6: Construct packet P, and do value assignment for □and□ $\square\square^B(t) \mid \square^B(t), \square^B(t) \mid \square^B(t), \ldots \square^B(t) \mid \square^B(t)\square$

7: Select B as the next hop which B meets access time is the minimumand nearer thesink //B is the node that is the longest time undetected and nearer the sink $\square^B(t) \mid \square^B(t)$ refers to the trust value of A to B at t (if data are dropped, then $\square^B(t) < 0$; otherwise, $\square^B(t) > 0$).

8: Send packet P to nodeB**Definition 1** (**Nodal direction trust**): Consider the trust set of

9: **End** for

10:**For** each node that receives a detection packet, such as node B, Donode A to node B during t to be: $\square\square^B(t) \mid \square^B(t), \square^B(t\ ) \mid \square^B(t), \ldots \square^B(t) \mid \square^B(t)\square$

11:let P. □=P. □-1, P.□=P.□-1

12:If □=0 thenThen, during period t , the total direction trust of A to B is:

$\square_B$

13:Construct feedback packet q, and do value assignment for each part $\square CA\square\square\square\square\square A(t_i)|\square A(t_i)\square\square(i)\square$ (6)

14 : Send feedback packet q to the source $i\square 1$ $\square_w$, $w \square 0$

15 : **End** if□0,$w \square 0$

16:

17:

18:**If p**. □□0 then

detection routing continue

End ifIn Eq. (6), (*i*) □[0,1] is an attenuation function toweight ħ

direction trusts at different times; according to common sense, the latest behavior should be given more weight [24],and

19:**End** for

20:**For** each node that receives feedback packet q, such as node C, Dootherwise less weight. The attenuation function is as shown in Eq. (7), and □is a decimal less than 1.

21:

22:

23:**If** q.destination is not itself then

send q to the source node

End if(*i*) □□ ħ { ħ ħ

□

1,

(*i* □1) □□*i* □*w*

(7)

(*i*), 1 □*i* □*w*

4:**End** for

This section details the implementation of the active detection routing protocol. The content of the detectionrouting packetcanbedividedinto6parts,asshowninFig.2:(a)packet head; (b) packet type; (c) ID of the source node; (d) maximum detection route length; (e) acknowledge returnedto the source for every □hops; and (f) ID of the packet.IntheActiveTrustscheme,thetrustcalculationshouldmeet the following condition. If the node is found to be malicious in the latest detection, then its trust should be below thethreshold □, and the node will not be chosen for later routing. If the malicious node returns to the normal node, it needs several detections to take it into routing consideration; thus, the parameter □should meet the following equation:

eorem 1: Consider that there are at most *w* interactionsC^T□□C^B□□1□□□□U^B(13)

involved in the trust computation and that the threshold is □; then, the parameter □should meet the following equation:

A,*B* *A* *A*

The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates

□□1□□^{w}□□1□□□□□1□□□^{B}□□□□^{B}(8)the direction trust according to Eq. (6) for each received feedback packet. Through interactions, the node obtains the

Proof: If the node is shown to be malicious in the latest

detection, then we can obtain □^{B}(*t*) <0; if it was shown to be trustable in the previous *w*□1 detections, then the trust of node A to node B must meet the following formula:

□^{B}+□□^{B}□□^{2}□^{B}□ …+□$^{w□1}$□^{B}□□

□□1□□^{w}□□1□□□□□1□□□^{B}□□□□^{B}

If there is more than one malicious result in the previous

$w-1$ detections, the trust should be less than α, thusproved.

■ **Inference 1**: If the node is shown to be malicious, then whenit returns to normal, there must be at least αtrustabledetections,

and it can be re-considered a trustable node; αmeets the following:

$1-\alpha-\alpha-\alpha\ldots\ \alpha\alpha^{\alpha-\alpha-1}\alpha\alpha^{\alpha}\alpha\alpha\alpha^{\alpha-\alpha-1}\alpha\ldots_{A}\alpha\alpha^{w-1}\alpha\alpha\alpha^{B}$ (9)

Proof: Consider that a node is shown to be trustable in the recommendation trust fromits neighbors according to Eq. (10), anditthencalculatesthemergedtrustaccordingtoEq.(12)for the multiple-recommendation trust. Finally, it calculates the comprehensive trust according to Eq.(13).

D. Data RoutingProtocol

The core idea of data routing is that when any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the preset threshold as the next hop. If the node cannot find any such appropriate next hop node, it will send a feedback failure tothe upper node, and the upper node will re-calculate theunselected node set and select the node with the largest trust as the next hop;similarly,ifitcannotfindanysuchappropriatenexthop,it sends a feedback failure to its upper node. The protocol is as follows:

Table 3: Pseudo-code of Algorithm 2 for data routing protocol

current αdetections, that is, $\alpha^{B}>0$, and malicious in the later

detection, namely, $\alpha^{B}<0$. Additionally, in the previous $w-1$ detections, the behaviors were all trustable. In this situation, αistheminimum,andthetrustofAtoBatthistimeisasfollows:

$\alpha^{B},\alpha_{A}\alpha^{B}{}_{A},\ldots,\alpha^{\alpha-\alpha-1}{}_{A}\alpha^{B}{}_{A},\alpha^{\alpha-\alpha}{}_{A}\alpha^{B},\alpha^{\alpha-\alpha-1}{}_{A}\alpha^{B},\ldots,\alpha^{w-1}\alpha^{B}$

The trust calculation is

$\alpha_{A}^{B}\alpha\alpha_{A}\alpha^{B}\alpha\ldots\alpha_{A}\alpha^{\alpha-\alpha-1}{}_{A}\alpha^{B}\alpha\alpha_{A}^{\alpha}\alpha^{B}\alpha\alpha^{\alpha-\alpha-1}{}_{A}\alpha^{B}\alpha\ldots\alpha\alpha^{w-1}\alpha^{B}\alpha\alpha$

Considering that $\alpha^{B}(t)=\alpha\alpha^{B}$, the above can betransformed

Algorithm 2: Data Routing Protocol

1: **For** each node that generates or receives a data packet, such as node A, Do 2: select B as the next hop such that B has never been selected in this data routing process, has the largest trust and is nearer the sink

4: **If** A finds such node, for instance, nodeB 5: Send data packet P to nodeB

6: **If** node B is the sinkthen

7: this data routing procession iscompleted

into$A$ i A

$1-\alpha-\alpha-\alpha\ldots\alpha\alpha^{\alpha-\alpha-1}\alpha\alpha^{\alpha}\alpha\alpha\alpha^{\alpha-\alpha-1}\alpha\ldots\alpha_{A}\alpha^{w-1}\alpha\alpha\alpha^{B}$ **End** if 9 : **Else**

10: Send failure feedback to the upper node, such as nodeC

■ 11: **End**if

Definition 2 (Nodal recommendation trust): Node A is the trustevaluator,nodeCisthetargetofevaluation,andnodeBis a recommender of A. Consider $C_{B}^{B}$to be the direction trust of A12:**End** for

13:**For** each node that receives failure feedback, such as node B, Do 14: Repeat step 2 to step 11 to B and C_{B}^{C} be the direction trust of B to C; then, the15:**End** for

recommendation trust of A to C is

$R^{C}\alpha C_{A}^{B}\alpha C_{A}^{C}{}_{B}$

(10)

E. The Number of Active DetectionRoutes

For the trust of multiple recommendations, the calculation of therecommendationtrustfromAtoB,BtoC,etc.,untilDtoE isFirst, we analyze the energy consumption at different distances from the sink. As in theorem 1 of Ref. [16], consider the network radius to be R , the nodal transmission radius to be

R^E □ C_A^B □ C_B^C □ C_C^D □ C_D^E

11)r , and the event generation rate to be □; the shortest route path protocol is deployed such that the nodal distance to the

Definition 3 (Recommendation trust merging): Consider thattherecommendersetofnodeAisR_A,$n_i \in R_A$ andthat

ink is l , $l = hr$ □x . The number of data packets undertaken by this node is thus as follows: the recommendation trust of n to node K is R; then, the d = (14)

iA□□□□□□□□ merged trust of A to K is

$R^{n_i,k}|$ z is an integer that makes l □zrjust smaller than R

U^K□□□$uR^{n_i,k}$□μ□ □□A (12)From Eq. (14), the energy consumption depends on the

A

n_i □An n_i An_i□$R^{n1,k}$□$R^{n2,k}$□...□$R^{nm-1,k}$□$R^{nm,k}$□

undertaken data amount. Thus, this paper considers the nodal

efinition 4 (Comprehensive trust): Comprehensive trust is the total trust, which merges the recommendation trust and direction trust:data amount to represent the nodal load. Because the network lifetime depends on the node that has the highest energy consumption, we consider the maximum nodal data load to be

maxand the energy consumption to be$d$max $e_u$and thusenergy to process detection routes without affecting the

observe that there is remaining energy for nodes whose data load is smallerthan$d$; then, we can fully use theremaining network lifetime.

Theorem 3: If the detection route length is □hops and one

max

energy to construct detection routes. For the node whose distance to the sink is l , the remaining energy of the node isdetection feedback packet is returned to the detection source

every □(□□□) hops, then the total number of detection hops in this route is

($d_{\max}$ □d_l)e_u,whichcanbeusedfordetection.Ifthedistanceof

an active detection route is measured by hops, then the $\hbar_{\varpi,\omega} = \sum^{i}$ /

k □1

k□□2□|i□□□□□□□(15)

available nodal hops of the active detection route is as follows: **Theorem 2**: If the nodal distance to the sink is l , then the maximum detection hops that can be achieved by its residue energy is $\hbar_l$ = □($d_{\max}$□d_l)(1□□$_2$)□/(1□□$_2$/ □$_1$) , where □$_1$ is theratioofdatapacketlengthtodetectionpacketlengthand□$_2$

is the ratio of data packet length to head packet length.

Proof: According to Eq. (14), for a node whose distance to the sinkis$l$,itsdataloadisd_l□□□z□1□□□z□1/z□r□2l□□.The maximumnodaldataloadis$d_{\max}$□□□z□1□□/□z□1□z□r□2$l_{\min}$□□.**Proof**: Because the detection data route length is □hops, the number of data route hops is □. One detection feedback is returned every □hops for a route with length □, and feedback is returned at □, 2□,... i□,□, where i□□□. The number of hops

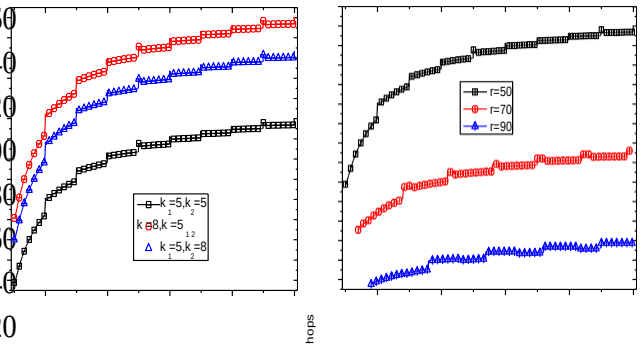
for each returned feedback is □, 2□,... i□,□;
the number of returned packet hops is thus □k□□□. Because
k □1
the route length is □and because it is possible for part of the
route to be unable to be created or for returned packets to be unabletoreachthedetectionsourceduetomaliciousnodes,the
i

Thus, the residue energy of this node is $(d_{\max} \square d_l)e_p$, where e_p denotes the energy consumption for sending and receiving a unitdatapacket.Consideringthattheenergyconsumptionfor
sending and receiving one bit data is e_u , e_p = □e_u because □is
the unit packet length, □= □$_h$ □□$_b$, □$_h$ is the packet headlength,maximum number of detection hops is
□k□□ 2□.
k □1
■
In summary, the number of detection routes that can be
created by residue energy can be found via Inference 2.
Inference 2: For a node whose distance to the sink is l , where
and □$_b$ is the packet body length. Then, the available residuethe detection route length is □hops and one detection
energy is $(d \square d)e$ (□□□)because the energyfeedback packet is returned to the detection source every □
max$l$ u h b(□□□) hops, the number of routes created by the residue
consumption for sending and receiving one detection packet is
e (□□□) ,where □ istheheadpacketlengthoftheenergy is
u h b h
□$(d \square d)(1 \square \square)$ □□^{i}□□□□
detection packet and □is the body packet length.Consider □ $= \square \frac{\max \; l \qquad 2}{} \square\square\square k \square \square 2 \square \square |$
i□(16)

b □,□$_{\square}$(1□□2 /□$_1$)□□k □1□ □□□□

□$_h$ to equal □$_h$, namely, □$_h$ = □$_h$, □$_b$ □□1□$_b$, □$_b$ = □2□$_h$.
Then,theactivedetectionroutehopsthatcanbeachievedby the nodal residue energyis
□d)e_l =(□$d_{\max}$□□) □e (□□□/)□**Proof**: According to theorem 2, for a node at a distance l from the sink, the maximum detection hops that can be achieved by its residue energy is = □$(d_{\max} \square d_l)(1 \square \square_2) \square /$ $(1 \square \square_2 / \square_1)$;
l u h b u h b
□ $\hbar_l$ =□(d /
□d)(1□□)□(1□□/ □)theorem 3 shows the maximum number of detection $\hbar_l$ hops to be
■ i

540
520
500
480
460
440
420
400
380
360
340
320max *l*2 2 1

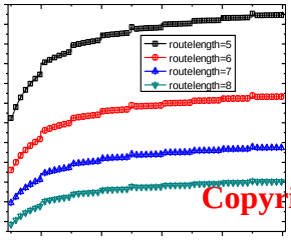


220□*k*□□ 2□. Thus, the number of detection routes can be
k □1
obtained by dividing thesetwovalues. ■

Inference 3: The ActiveTrust scheme has the same network lifetime as do schemes without any security strategy.

Proof: The ActiveTrust scheme uses residue energy to construct detection routes; this construction energy consumption will not make the nodal energy consumption larger than *d* , and thus, its lifetime is still □= *E d* . /

300
280
100 200
300
400
500200
180
100 200
300 400 500
30
max



*init*max

■

distancefromsink(m)distance from sink

28

26

24

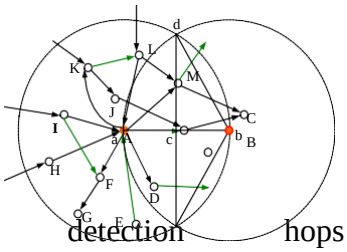
22

20

Fig. 4 The maximum detection hops afforded by the residue energy of nodes (different k_1, k_2)

Fig. 5 The maximum detection hops afforded by the residue energy of nodes (different r)

The number of probing routes



Figs. 4 and 5 provide the maximum detection hops affordedbytheresidueenergyofnodeswithdifferentdistances from the sink. As seen, there is much residue energy in non-hotspots because the detection packet length is small; in a network with radius R =500 m, the detection hops cannumber

18

16

14

12

10

8

100 200

300 400 500

in the hundreds, which shows that the network has sufficientdistance from sink (m)

Fig. 6 The number of probing routes that can be created

Fig. 7 Indirection trust among nodes

ig. 6 shows, in a network with radius R =500 m, the number of probing routes that can be created by residue energy in non-hotspots under detection route lengths of 5, 6, 7, and 8. As seen, the residue energy can support at least 7 detection□=□(2□□3)*d*□2□*m d*;thisalsoappliestonodeB.The

□3 2□ □*d*

probabilities of these two sets are completely different, that is,
routes. Performance Analysis of the ActiveTrust Scheme

F. Analysis of the Successful RoutingProbability□*p* □ 0

□ $c^v.c^v$

(□□*v*)!(□□*v*)!*if* □□ 2*v*

□*p* □□□□*v*□

if □□ 2*v*

μμ

Theorem 3: Considering that the nodal degree is d , after one round of a detection route whose length (number of hops) is x , thenumberofnodesthathavedirectiontrustism_d,thenumber of nodes that have a minimum indirection trust is m_{in} , and the number of nodes that cannot obtain trust is m_{no} ; theyare

m□□1□(1□□)^x□□,m□(1□P)d,m□(d□m)P|m□d(17)□ $c^v.c^v$ □!(□□2*v*)!

Therefore, the probability that A cannot obtain the indirection trust of B is P , A has d neighbors, among which there are m_d nodes that can obtain direction trust and m_{in}=(1□P)$d$nodesthatcanobtainindirectiontrust,andthe number of nodes that cannot obtain trust is
d *in* *no* *d*

where $m_{no} \square (d \square m_d)P \mid m \square d$.

□

□$p \square 0$

□$if \square\square 2v \mid \square\square (1\square^3)d \square 2$ $\sqrt{\quad}$

2□

■

Theorem 4: If only direction trust is considered, and the numberofsuchnodesis$m$,thenthesuccessratefordata

□ $(\square\square v)!(\square\square v)!$ $\square\sqrt{3}$ □ d

□$p \square if \square\square 2v \mid \square\square_{\square}(1\square$ $)d \square 2 _ m_d d$packets sent to the sink by nodes that are k hops away is

□□ $\square!(\square\square 2v)!\square$ 2□ $\_\square\square^k\square(1\square\square d3)^{k\square 1}$ $if m \square d$

Proof: Considering that the malicious node ratio is □, the $\square d$ d (19)

$\square\square^k\square(1\square\square md3\square 1)k\square 1 if\ m \square d$

detectionroutelength(numberofhops)is$x$,thoughduringthe routing, it may end early due to a black hole. Then, for route length x , the actual average route length is calculated as follows:

The probability of encountering a black hole at the first time is □, and the probability of not encountering one until the second time is $(1\square\square)\square$; thus, the probability of not encountering one until the i th time is $(1\square\square)^{i\square 1}\square$. Thus, the actual average route length is

$m \_\square\square\ 2(1\square\square)\square\square ... \ \square i(1\square\square)^{i\square 1}\square\square ... \ \square x(1\square\square)^{x\square 1}\square(18)\square d\ d$

Proof: First, calculate the success rate of any of node A's one-hop transmissions. A failed transmission means that node A finds that all of the detected nodes whose hops smaller than itselfareblackholes;thedetectednodescannotbeselected,and A must select from the undetected nodes. If the selected undetected node is a black hole, the transmissionfails.

Thus,thefailureprobabilityisasfollows.Thereare3states for node A, that is, nodes whose hops are larger than, the same as and smaller than A's. For the nodal degree d , the number of nodeswhosehopsaresmallerthanA'sis$d3$,andthereare

After complex processing, the above equation can be simplified into: $m \square\square 1\square (1\square\square)^{x}\square\square$.

If each node processes one round of detection with length x, then from the average, it is equivalent to for each node to process m_d detection routes to its neighbors; thus, thenumber

of nodes with direction trust is m_d.

Forindirectiontrust,asshowninFig.7,nodeAandnodeB have a minimum number of common neighbors; then, the indirectiontrustprobabilityistheminimumitcanbecalculated as follows:

The number of common nodes of A and B is the number of nodes within the same transmission radius. The area of this

region is $2(\square r^2 3\square r)^2 = 2\ \square\sqrt{r^2}\square^3 r^2$. m_d 3 detections for these smaller nodes, with a total of m_d detections.

If $m_d \square d$, then all of the neighbors of node A can be detected; then, only if all of the next hop nodes are blacknodes canthedatatransmissionfail;theprobabilityofthissituationis

$\square = \square^{d 3}$.

If $m_d \square d$, the black node probability for each detection is $\square^{m_d 3}$,andtheblacknodeprobabilitywhenchoosingthenext hop is $\square^{m_d 3\square 1}$; that is, the failure probability is $\square = \square^{m_d 3\square 1}$.

Therefore, for a node at k hops from the sink, if data are

sent k hops and the last hop is not a black node, then the success transmission probability for each hop after that is

$\square\square^{k}\square(1\square\square^{d3})^{k\square 1}$ $if m\square d$

2 2 3 $2^{\square}\square^{k}\square(1\square\square^{m3\square 1})^{k\square 1} if\ m\ \square d$

The number of nodes in this region is

$(\frac{2}{\square}r^2\square\frac{3}{2}r^2\sqrt{\square}\square\square\frac{2}{\square}r^2\square\frac{3}{2}r^2\sqrt{\square}d\square\square r^2\square$.

$\square\square d$ d d

■

3 2 \ $\square 3$ 2/ $\square$

Except for A and B, the number of common neighbors

is$\square=(^{2}\square\frac{\sqrt{3}}{\ }\ )d\ \square\ 2$.**Inference 4**: Considering that the number of nodes with direction trust is m_d and that the number of nodes with

indirection trust is m_{in}, the success ratio for nodes at k hops

from the sink is

3 $2\square$

$m\square\square\square^{k}\square(1\square\square^{d3})^{k\square 1}$ if $|m\ \square m|\square d$

Node Aprocessed $d$detections, and then the number $\square di$ d $in(20)$

$\square\square^{k}\square(1\square\square(m_d\square m_{in})3\square 1)^{k\square 1} if\ |m\ \square m\square d$

of detections for the common neighbors is $\square di \quad d \quad in$

Proof: Because the indirection trust is within a range of two hops, the black node can be identified with indirection trust, and thus the number of recognizable nodes is the union of

1.0
0.9
0.8
0.7
6.5
6.0
5.5
5.0
direction and indirection nodes, that is, $|m \square m|$; therefore,0.6
4.5
$d \quad in$
Inference 4 can be inferred from Theorem 4.0.5
0.4
■ 0.3
0.2
4.0
3.5
3.0

Theorem 5: If only direction trust nodes are considered, and the number of such nodes is m_d , then, for a network whose $R \square hr$, the success ratio is

$\square h \qquad d\ 3k \square 12^{-}$
0.1
0.0
0.02 0.04 0.06 0.08 0.10 0.12 0.14 0.16
□
0.18
2.5
2.0
5
10 15 20 25 30
d

Fig. 8 Total data route success ratio

Fig. 9 Required network scale that makes the number of detected nodes larger than the nodal degree without affecting the network lifetime

$\square \square \square (2k \square 1)(1 \square \square \quad)$
$\square = \square^{k \square 2}$
$_{d} \square h \quad if\ y \square d(21)$

$\square \square \square^{h} (2k \square 1)(1 \square \square^{y\ 3 \square 1})^{k \square 1} \square h^{2}$
$\square k \square 2 if\ y \square d$According to theorems 3-5, if the number ofdirection detection nodes is larger than the nodal degree, which means thatallneighborsaredetectedandallneighbortrustisobtained,

Proof: Theorem 4 gives the success probability $\square^{k}$ fornodes at k hops from the sink because the number of such nodes at

k hops is $\pi[(kr)^2-((k-1)r)^2]=\pi(2k-1)r^2$.
Then, the number of nodes whose data successfully reaches the sink is $S=\pi(2k-1)r^2$ only a scenario in which all neighbors are black nodes can cause the transmission to fail. In fact, if this happens, no scheme can solve this problem because all paths to the sink are blockedbyblacknodes.Therefore,thesituationinwhichthe numberofdetectednodesequalsthenodaldegreeisoptimal.Inthefollowing,weanalyzewhetherthisidealsituationc anbe

k d

Because there is no black node within a one-hop range, the total number of packets that successfully arrive at the sink is

$$S_{total}=\sum_{k=2}^{h}(\pi\rho(2k-1)r\chi)=\pi\rho r^2\sum_{k=2}^{h}(2k-1)(1-d)^{k-1} \quad if\ y=d$$

achieved in WSNs.

Theorem 6: For nodal degree d and feedback that is returned hop-by-hop in the detection route, if the network scale meets the following equation, the number of detected nodes can be larger than the nodal degree without affecting the network lifetime, thereby achieving maximum security.

$k=2$
h

$h=$ (23)

$$\pi r^2\sum_{k=2}^{h}(2k-1)(1-md\ 3-1)^{k-1} \quad if\ m=d$$

d

$k=2$

and the number of packets sent in the entire network is $\pi(hr)^2$. Thus, theorem 5 can be proved.

■ Fig. 8 shows the total data route success ratio with our scheme (only one detection route with a length =5). As seen, our scheme has a much higher total success ratio than does the shortest routing scheme.

Inference 5: Considering that the number of nodes with directiontrustis$m_d$andthatthenumberofnodeswith**Proof:**(1)Theenergyconsumptionisthehighestinthe1st ring, and the second highest is the 2nd ring. Thus, if the energy can afford the 2nd ring to detect nodes d , then other rings can ensure that the detected nodes d . The data load in the 1st ring is $h^2r^2\pi$, and there are $r^2\pi$ nodes in the 1st ring; then, the data load for each node is $h^2r^2\pi/r^2\pi=h^2$. Considering thattheenergyconsumptionforsendingaunitdatapacketise_u, the energy consumption in the 1st ring is h^2e_u .
There are $2^2r^2\pi-r^2\pi=3r^2\pi$ nodes in the 2nd ring,

indirection trust is
$m_{in}$for a network whose $R=hr$, the successful data transmission ratio in our schemeis

□ *h*
□ □(2*k*□1)(1□ □*d*3)*k*□1□*h*2 *if*|*m*□*m*

|□*d*andthedataloadis(□*h*2*r*2□□□*r*2□),so thedataloadforeach node is □□*h*2*r*2□□□*r*2□□3□*r*2□= □*h*2□1□*e* 3 ; thus,the

□*k* □2
di *hd* *in*
-22)remaining energy in the 2nd ring compared with that in the 1st ring is h^2e - □*h*2□1□*e* 3 = □2*h*2□1□*e* 3 . *e* is the energy

□ □ □(2*k*□1)(1□□|*md*□*min*|3□1)*k*□1□*h*2*if* |*m* □*m*|□*du* *u* *u* *p*

□*k* □2*d* *in*consumptionfor a detection packet, so

Proof: Similar to inference 4, inference 5 can be inferred from theorem 3.e_u □(1□□2) (1□□2 / □1) *e p* can be used for detection packets, and the number of detection packetsis

■

□□2*h*2□1□3□□(1□□)(1□□/□)□
2 2 1

If the detection route length is *x* , then the number of nodes that can be detected is *md* □□1□ (1□□) □□. If *m* □*d* ,
x
d
then there should be at least *n*min □*d md*detection routes.

□□1□(1□□)*x*□□,*m*□(1□*P*)*d*,*m*□(*d*□*m*)*P*|*m*□*d*□*r*2□□□(2*k*□1)(1□□)*k*□1□ □□(2*k* □1)(1□□)*k*□1□
d *in* *no* *d* *h* *h*

For a detection route with length *md* , the number of detection packets needed is

k□2 □*k*□2
□□(*hr*)2 *h*2

1+2+3…+ *md* + *md* = □*md* 2□ 3*md* □2Therefore, the packet success ratio of our scheme to the shortest route scheme is

The total number of needed detectionpacketsis *h*

*n*min□*m* 2□3*m* □

2 = □(1□ (1□□)*x*□6□)*d* □□2□□□□□□*h*2□□(2*k* □1)(1□□)*k*□1□
k □2 *d* *d* *d*

because

□□□2*h*2□1□3□□(1□□2)(1□□2/□1)□□□□(1□(1□□)*x*□6□)*d*□□2□□□
□*h* >*h* □

■

AsseeninFig.9,ifthenetworkscaleisonly7hopswith anodaldegreeof30,theresidueenergyinnon-hotspotsregion can process a sufficient number of detection routes in one roundofdatacollectiontodetectallneighbors'trustwithout■

Figs. 10 and 11 show the improved ratio of our schemeto theshortestroutescheme.Asseen,asthedistancefromthesink increases, more hops are required for data to be transmitted to thesink,sothesuccessratiointheshortestrouteschemeislow; however, our scheme is based on the detected nodal trust, and the success probability is higher because of the selection of high trust nodes. If the black node ratio is higher, it is more improvedbyourscheme(upto10timesmore),thusconfirming the effectiveness of our scheme (see Figs. 10 and11).

16

affecting the network lifetime. This state achieves the best security.

Theorem 7: For nodes that are k hops away from thesink,the success ratio of our scheme when the shortest routeisadopted is

6

20

$\beta_k = \chi_k(1-\beta_k)^k(1-\beta)^k$

24)

2

Proof: For a black node ratio in the network of and for nodes that are k hops away from the sink because nodes are randomlyselected,theprobabilityofablacknodeisthesame0

5 10 15 20 25 30

Distance from sink (hops)

0

0.02 0.04 0.06 0.08 0.10 0.12 0.14 0.16 0.18

as the black node ratio in the network, that is, , for each hop selection. The last hop is not a black node; thus, with the shortest route scheme, the probability of all non-black nodes being selected after k hops is $(1-\beta)^{k-1}$, and the ratio of our scheme to the shortest route scheme is

$\beta_k = \chi_k(1-\beta_k)^k(1-\beta)^k$

Analysis of the EnergyEfficiency

This section analyzes the energy efficiency performance of our scheme and compares it to other schemes.

Theorem 9: If each node, except for nodes in the 1st ring, processes n_a detection routes with length x , then the energy efficiency is

■ h m^2 $3m$

d $d_e 1-(1-\beta)^k$

1 2 2

Theorem 8: In a network whose $R = hr$, the success ratio of our scheme to the shortest route is=

$k2 e(2k1)$

1 $h e_u h$ (26)

h

$1-(1-\beta)^x n3-1 \quad d3$

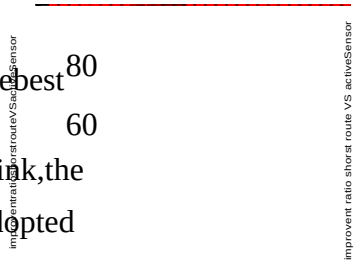


Fig. 10 Improved ratio of our scheme to the shortest route scheme

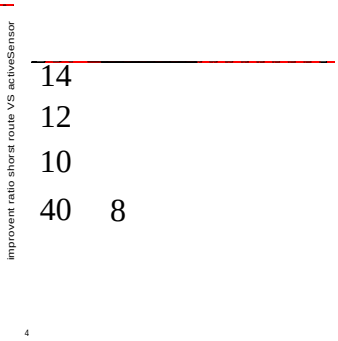


Fig. 11 Total improved ratio of our scheme to the shortest route scheme

d 2 p

ς p

$1-(1-\beta)^x$

□□□□h^{2} $_{d}$

□□(2k □1)(1□□)$^{k□1}$□(25)| n_{d}□ min □n_{a}□ ,d□,m_{d}□□ ,□1 □□d |□

k □2

Proof: The above theorems have proved that in the shortest route scheme, the success probability of data at k hops to the sink is (1□□)$^{k□1}$. In the network, the number of nodes that are$k$ hops from the sinkis □□□(kr)^{2}□□((k □1)r)^{2}□□□□(2k □1)r^{2}□ □

Proof: According to theorem 1, the number of nodes whose direction trust can be obtained in one detection route with
length x is m □□1□ (1□□)^{x}□□□1□ (1□□)^{x}□□; after n $_{d}$ | | $_{a}$
detection routes, the number of nodes whose direction trust can be obtained is n = min□n □1□(1□□)^{x}□□, d□. Theorem 4
$_{a}$ $_{a}$ |

Thus, in the shortest route scheme, the number of successfulndata packets at k hops to the sink is provedthatforadetectionroutewithlengthm_{d} ,thenumber
of detection packets is □m ^{2}□3m □2 ; thus, for n detection |

S□□□(2k□1)r^{2}(1□□)$^{k□1}$$d$ d a

k routes, the number of detection packetsneeded is

There is no black node in the 1st ring; thus, in the entire network, the number of packets to the sink is$n$ □m ^{2}□ 3m □2 . Theorem 2 proved that the number of nodes $_{a}$ $_{d}$ $_{d}$
n
h whose direction trust is available is$_{d}$and that the
probability

S_{total}□□□□□(2k □1)r^{2}(1□□)$^{k□1}$□of data failure for the next hop is □$_{1}$□□$^{nd\ 3□1}$ | □$^{d\ 3}$. Therefore,
□2

There are □□(hr)^{2} nodes in the network, so the packet success ratio in the entire network isfor nodes that are k hops from the sink, the number of average data route hops is □1□ (1□□)^{k}□□.

us, the energy consumption of a node that is k hops from the sink is

500

450

425

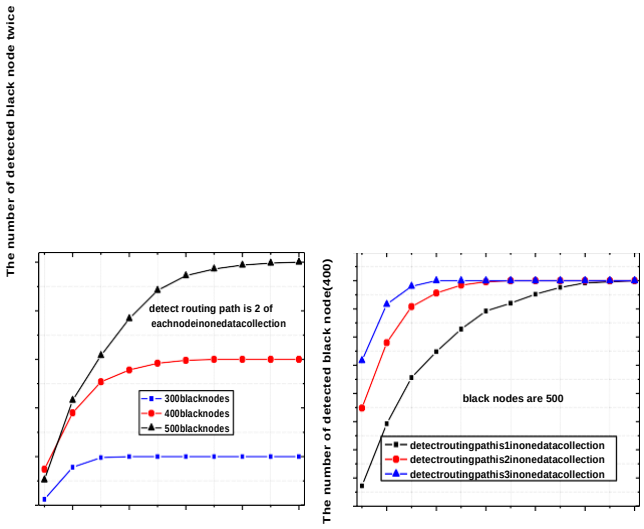
400

375

n n □m ^{2}□ 3m □e 2 □□1□ (1□□)^{k}□e □e .

350

d d d d p



1 1 *p*

400

325

Because there are □□(2*k* □1)*r*^{2} nodes that are *k* hops from the sink, the total energy consumption is

350

300

275

h□□*m* ^{2}□3*m*1□(1□□)^k □□ 300250

□□□*n*_dd *d*_*e*□□1 *e* *p*□□□□(2*k* □1)*r*^{2}□□

250

225

200

k□2□□□1 □ □□2 4 6 8 102 4 6 8 10 12

an the highest energy consumption is $h_u^2 e$. Then, the

Fig. 14. The number of detected lack nodes as the network operates

Fig. 15. The number of detected nodes in one data collection round under different numbers of detection routes

time(rounds)time(rounds)

energy efficiency of our scheme is

$$\eta = \frac{h\,n_d\,3m_d\,e}{1-(1-1)_e}$$

$$\frac{m(2k-1)\,h^2 e\,h^2}{d\quad p\quad p}$$

$$k\,2\quad 2\quad 1\quad u$$

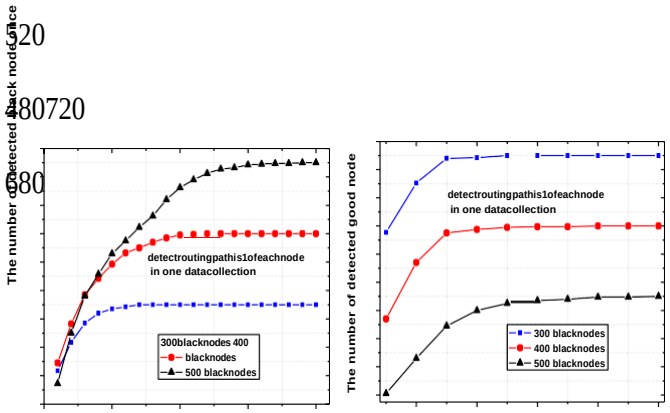
Fig. 14 shows the number of black nodes detected ineach

datacollectionwithtwicedetecting.Asseen,comparedwith once detecting, the black node detection speed doubles, andall black nodes can be detected in, at most, 7 rounds. The

V. EXPERIMENTALRESULTS

The experimental platform adopted in this paper is OMNET++ [37]. Unless otherwise noted, the experiments use the following settings. The network radius R =500 m, there are a total of 1000 nodes in the network, among which there are 300 black nodes, nodes are randomly and uniformly deployed, and the sink is at the network's center.

*A. Experimental Results of Node Trust*experiment in Fig. 15 further illustrates this problem, which shows that the more detection routes there are in one data collection round, the less time is needed to detect all of the black nodes. This indicates that the black nodes can be more quickly detected as the detection grows, which improves network security. According to inference 2, the residue energy innon-hotspotscanafford7times(orevenmorethan10times) detecting; if all of the residue energy is used to construct detectionroutes,thesystemcandetectalmostalloftheblack

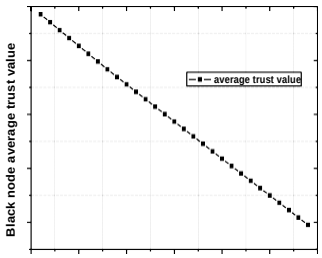


nodesinatmosttwodatacollectionrounds,whichfullyverifies the fast recognition ability of ourscheme.

440
400
360
320
280
240
200
160
0 5 10 15 20
time (rounds)640
600
560
520
480
440
400
360
2 4 6 8 10
time (rounds)0
-1
-2
-3
-4
0 5 10 15 20 25 30
time(rounds) 3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
0 5 10 15 20 25 30
time(rounds)

Fig. 12. The number of detected black nodes as the network operates

Fig. 13. The number of detected good nodes as the network operates



Normal node average trust value

TheexperimentalsceneinFig.12issuchthatineachdata collection round, each node initiates one detection route with a lengthof5.Asseen,asthenetworkruns,i.e.,asmoredetection routes are performed, the number of black nodes detected grows quickly; when the number of deployed black nodes is 300, 400 and 500, the time needed to detect them all is, respectively,5,9and12rounds,whichshowsthatthe

Fig. 16. Average trust ofblack nodes as the networkoperates

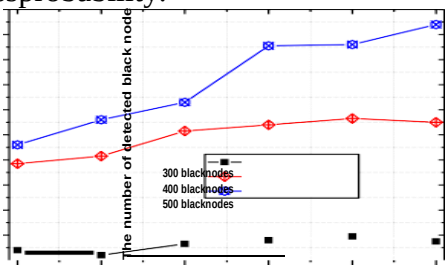
Fig. 17. Average trust of good nodes as the network operates

The experimental scene in Figs. 16 and 17 deploys 1000 nodes in a network with 400 black nodes. In each data collectionround,eachnodecreatesdetectiononce.Asseen,the average trust of black nodes declines as the network operates, whereas that of good nodesincreases.

480

ActiveTrust scheme can quickly detect malicious nodes within only several detections. Fig. 13 shows the number of detected goodnodesasthenetworkrunsinthesameexperimentalscene as in Fig. 12; as seen, after only 4 rounds, our ActiveTrust scheme has detected all of the good nodes because in the data routing, it needs only one good downstream node to route the next hop; this indicates that, according to our scheme, theroute can be reliable and have a high successprobability.

460
440
420
400
380
360
340
320
300
280
1200
1100
1000
900
800
700
600
500
400



1000 1100 1200 1300 1400 150(
Different node density

Fig. 18. The number of detected black nodes under different nodal densities

1000 1100 1200 1300 1400 1500
Different node density

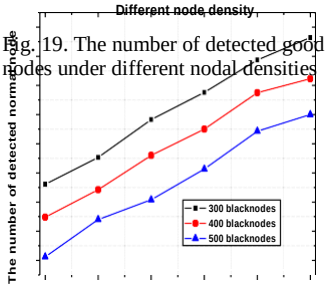


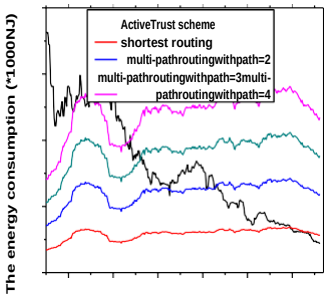
Fig. 19. The number of detected good nodes under different nodal densities

Figs. 18 and 19 show the number of detected black nodes or good nodes after two rounds of data collection when each node detects once in each round for a network of 1000, 1100,

1200,1300,1400,and1500nodeswith300,400,and500black nodes. As seen from Fig. 18, for a situation with 300 black nodes and a 90% detected black node ratio, the increase in the number of detected black nodes is smaller as the nodal density increases,butifthereare500blacknodes,thisincreaseismore obvious,whichshowsthatourschemehasgoodperformancein networks with greater nodal density. In Fig. 19, the number of detected good nodes grows as the nodal density increases, which shows that in networks with greater nodal density, the success route probability increases, which matches the actual situation.

B. Experimental Results of EnergyConsumption

800
600
400
200
0
50
100 150 200 250
distance from sink(m)



300
250
200
150
100
50
50 100 150 200 250 300

The energy consumption of sink
success to receive

distance from sink (m)

Fig. 24. Energy consumption comparison under different schemes

Fig. 25. Energy consumption for unit success under different schemes

Fig. 20 shows a 3-d map of energy consumption for each node detecting three times in one data collection round in a network with R =400 m and 400 black nodes from a total of 1000nodes.AsseenfromFig.21,becausethedetectionenergy consumptionisbasicallybalancingshared,exceptthedetection energy consumption near the sink is very low (to decrease the energy consumption in hotspots), the energy consumption is balanced in other regions; as the detection routes increase, the detection energy consumptionincreases.

Becausethedatasuccessrouteprobabilityislowandmost routes are blocked by black nodes in the shortest route scheme, the sink only receives a few data packets. Therefore, in this situation, the energy consumption is more balanced (see Fig. 22). In the ActiveTrust scheme, because the data success route rate is higher, the energy consumption near the sink is higher; althoughthereisdetectionenergyconsumptioninnon-hotspots, the detection energy consumption is low compared with data collection energy consumption, so the energy consumption near the sink is higher than that in other regions. A 3-d map of the energy consumption is shown in Fig. 23, which also indicatesthatthereissufficientenergyremainingfordetection.

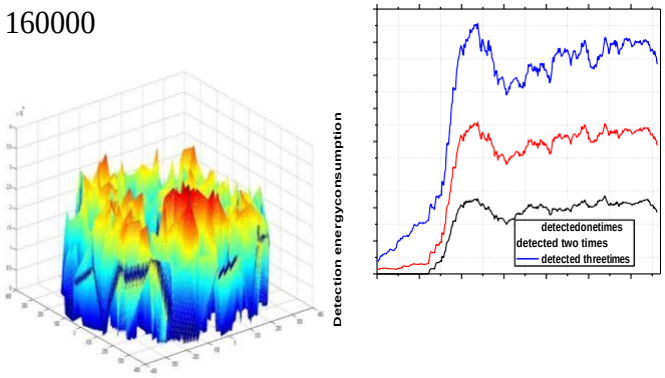


Fig. 21 Detection energy consumption at different distances from thesink

Fig. 20 Energy consumption for each node detecting three times in one datacollection round

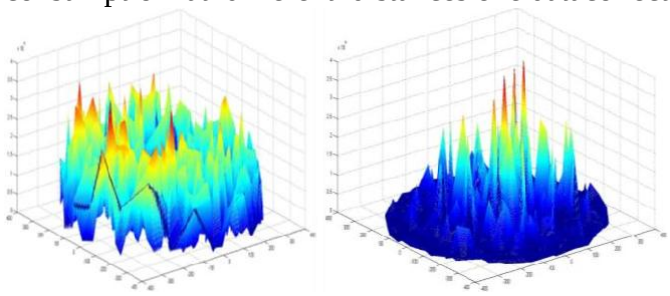


Fig. 24 shows the energy consumption at different distancesfromthesinkafteronedatacollectionround.Asseen, with the shortest routing, the energy consumption is less, as explained previously. With multi-path routing, i.e., one data packet is sent to the sink via different paths to improve the success rate, more packets reach the sink, and the energy

consumption is proportional to the number of paths, i.e., the more paths there are, the higher the energy consumption is and the higher the success rate is for data arriving at the sink. Although the success rate increases as the number of paths grows, there are some problems. (1) The success rate is not high; for instance, if the success rate for each path is 20%, then evenif10pathsarecreated,thesuccessratedoesnotreach90%.
(2) Even if a certain success rate is achieved, the network lifetime is affected. Therefore, in our scheme, by constructing light active detection routes, malicious nodes can be detected withoutaffectingthenetworklifetime,whichalsoimprovesthe success rate with goodperformance.
Fig. 25 shows the ratio of nodal energy consumption to the number of packets that are successfully routed to the sink. This ratio reflects that with the same energy consumption, the number of successful packet in different schemes does, in fact, indicate the network energy efficiency. As seen, our scheme can improve the energy efficiency by more than 2 times compared with that of previous researches which is consistent with theorem 9.

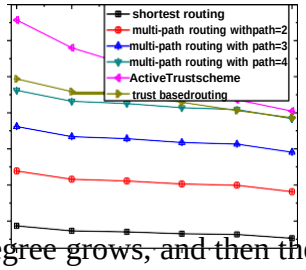
C. Comparison of the Probability of SuccessRouting

The experimental scene in Fig. 26 is a network with R =400 m and 400 black nodes from a total of 1000 nodes, whereeachnodeonlydetectsonce.AsseenfromFig.26,asthe network runs under our scheme, the probability of successful routing is almost 100% after 7 data collection rounds. For the shortest routing, this probability is not even 15%. With multi-path routing, it is only approximately 60% with 4 paths simultaneously. Moreover, in this black node avoidance scheme, no matter how long the network runs, the probability of successful routing will never increase. The trust-based routing is similar to the TARF scheme [30], in which the next hop is selected based on the trust of the node. Thus, the probability of successful routing will increase with time. However, the scheme does not detect nodes' trust actively, so its probability of successful routing is lower than that of the proposed scheme. Fig. 27 shows the probability of successful routing under different numbers of black nodes. As seen, our scheme is significantly better than multi-path routing. Fig. 28 showstheimprovementofourschemecomparedwithother

Fig. 22. Energy consumption with the shortest routing scheme

Fig. 23 Detection energy consumption at differentdistances from the sink

chemes; as seen, our scheme is better than other schemes. When the network runs a short time, the successful routing probability is improved from 1.5 times to 6 times. Fig. 29 shows the improvement of our scheme compared with other schemes under different numbers of black nodes. As seen, it is improved by more than 3 times compared with the shortest routing and is higher than multi-path routing schemes and trust-based routing.



density grows, the nodal degree grows, and then there aremore detected trustable nodes after detection, that is, there are more nodesforthenexthop,andtheprobabilityofsuccessfulrouting thus increases. Fig. 33 shows the probability of successful routing as the nodal transmission radius r grows; as seen, the probabilityofsuccessfulroutingisalsoincreased.Thereasonis that, as r grows, the nodal density grows, which is the same as found in the experiment of Fig.32.

1.0

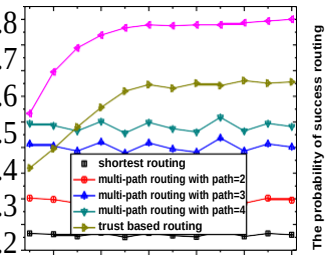
0.9

The probability of success routing

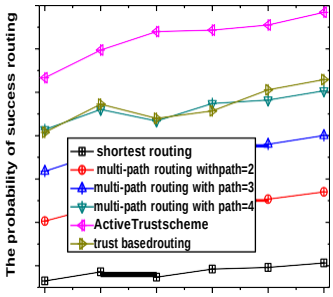
0.8

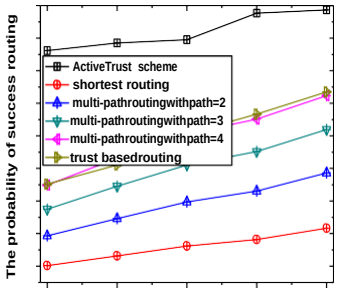
0.7
0.6
0.5
0.4
0.3
0.2
0.1

Time(rounds)



12
300 350
400 450 500 5500.8
0.7
0.6
0.5
0.4
0.3
0.2
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2





The number of black node

Fig. 26. The probability of successful routing as the network operates

Fig. 27. The probability of successful routing under different numbers of black nodes

Fig. 30 shows the probability of successful routing as the network runs under the ActiveTrust scheme; as seen, even in

1000 1100 1200 1300 1400 1500

Different node density0.1

80 90 100 110 120

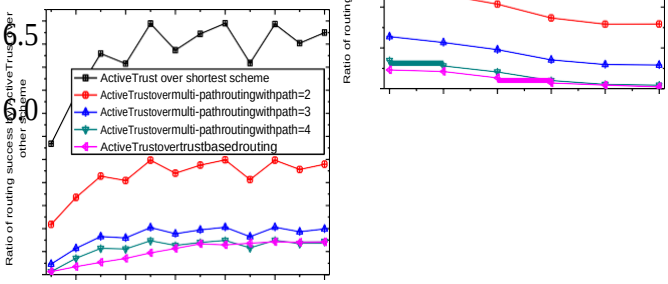
r(m)

Fig. 32. The probability of successful routing under different nodal densities

Fig. 33. The probability of successful routing under different nodal transmission radiuses r

the situation where there is only one detection in one data collection round, the probability can be almost 100% after several data collection rounds. Fig. 31 shows the probability of successful routing in one data collection round with one, two and three detections. As seen, if the detection routing path is 3, after only 3 rounds, the probability can be almost 100%, which verifies the high probability of successful routing in our scheme.

Figs. 34 and 35 give the probability of successful routingof the ActiveTrust scheme for different BLAs. In the experiment, the black hole attack refers to the malicious attack in which all data that attempt to pass by are dropped. However, the Denial-of-Service Attack refers to the attack in which data are droppedintermittently[35,36],thusmakingitdifficulttoresist this attack. The select forward attack is one of the most intelligent attacks and can drop data selectively [6]. It can be seenfromFigs.34and35thattheActiveTrustschemehas



positive effects on the different impacts of BLAs.

6.5
6.0
5.5
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
2 4 6 8 10 12
Time (rounds)
3.5
3.0
2.5
2.0

1.5
1.0
300 350 400 450 500 550
The number of black node1.0
0.8
0.6
0.4
0.2
0.0 3 6 9 0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
350
450
550

Fig.28Ratioofsuccessfulrouting
with different schemes as the network operates

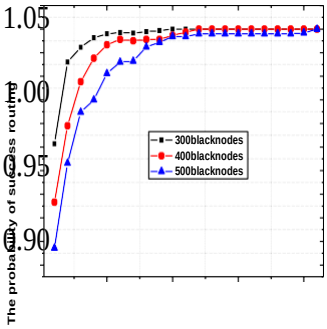


Fig. 29 Ratio of successful routing
with different schemes under different numbers of black nodes

1.0
0.9
Time (rounds)

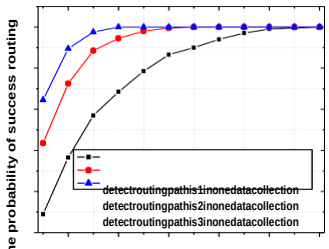


Fig. 34. The probability of successful routing for different BLAs

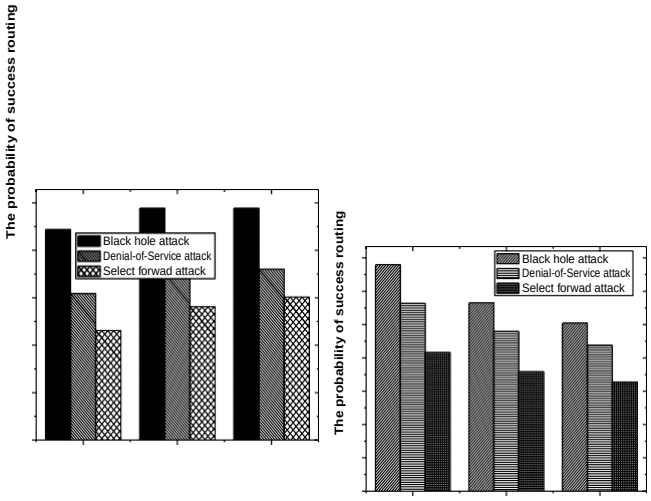


Fig. 35. The probability of successful routing under different numbers of black nodes for different BLAs

CONCLUSION

The number of black node
0.85
0.80
0.75
0.70
0.65
0.60
0.55
0.50

5 10 15 20
time (rounds)
0.8
0.7
0.6
0.5
2 4 6 8 10 12
time(rounds)

We proposed a novel security and trust routing scheme based on active detection in this paper, and it has the following excellent properties: (1) High probability of successful routing, security, and scalability. The ActiveTrust scheme can quickly detect nodal trust and then avoid suspicious nodes to achieve a near-perfect routing probability. (2) Extremely high energy efficiency. The ActiveTrust scheme makes full use of residue energy to build multiple detection routes. Theoretical and experimental results show that our scheme improves the success rate

Fig. 31 The probability of successful routing

Fig. 31 The probability of successful routing under different numbers of detection routing paths in one data collection round.

Fig. 32 shows the probability of successful routing under different nodal densities. As seen, when the nodal density grows, the nodal degree grows, and the probability of successful routing increases. The reason is that as the nodalrouting probability by more than 3 times, up to 10 times in some cases. Further, our scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

REFERENCES

a. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391,2014.
b. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks,"IEEETransactionsonParallelandDistributedSystems,vol. 27, no. 1, pp. 225-236,2016.
c. S. He, J. Chen, F.Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942,2013.
d. X.Liu,M.Dong,K.Ota,P.Hung,A.Liu."ServicePricingDecisionin Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198,2016.
e. C.Zhu,H.Nicanfar,V.C.M.Leung,etal."AnAuthenticatedTrustand Reputation Calculation and Management System for Cloud andSensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131,2015.
f. A.Liu,M.Dong,K.Ota,etal."PHACK : AnEfficientSchemefor
[2]. Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no.
[3]. 12, pp. 30942-30963, 2015.
a. A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences, vol. 230, pp.197-226,2013.
b. Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone DetectioninWirelessSensorNetworks,"IEEETransactionsonMobile Computing.vol. 15, no. 5, pp. 1130-1143,2016.
c. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954,2010.
d. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-EfficientTrust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625,2015.
e. S. Shen, H. Li, R. Han, et al. "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.9,

no. 11, pp. 1962-1973,2014.
f. O. Souihli, M. Frikha, B. H. Mahmoud, "Load-balancing in MANET shortest-path routing protocols," Ad Hoc Networks, vol. 7, no. 2, pp. 431-442,2009.
g. J. Long, A. Liu, M. Dong, et al. "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.
h. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282,2015.
i. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions onInformation Forensics and Security, vol. 10, no. 2, pp. 371-383,2014.
j. Y. Hu, A. Liu. "An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs," The Computer Journal, vol. 58, no. 8, pp. 1747-1762,2015.
k. S. J. Lee, M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," IEEE ICC, pp. 3201-3205,2011.
l. Y. Zhang, S. He, J. Chen. "Data Gathering Optimization by Dynamic Sensing and Routing in Rechargeable Sensor Networks," IEEE/ACM Transactions on network, doi:10.1109/TNET.2015.2425146,2015.
m. T. P. Nghiem,T.H.Cho,"Amulti-pathinterleavedhop-by-hopen-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, no. 10, pp. 1202-1209,2010.
n. Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of NetworkandComputerApplications,vol.35,no.3,pp.867-880,2012.
o. Q. He, D. Wu, P. K. Sori, "a secure and objective reputation-based incentive scheme for ad hoc networks," IEEE Wireless Communications and Networking Conference, pp. 825–830,2004.
p. S. Kamvar, M. Schlosser, H. Garcia-Molina, "The eigentrustalgorithm for reputation management in P2P networks," in: Proceedings of the 12thInternationalConferenceonWorldWideWeb,pp.640–651,2003.
q. H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, "Combining trust with location information for routing inwireless

[4]. sensor networks," Wireless Communications and Mobile Computing, vol. 12, no. 12, pp. 1091-1103, 2012.
a. J.Wang,Y.H.Liu,Y.Jiao,"Buildingatrustedrouteinamobilead hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1138-1149,2011.
b. H. Sun, C. Chen, Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, pp. 1-4,2007.
c. Z. Ye, V. Krishnamurthy, S. K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, pp. 270-280,2003.
d. W. Lou, Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Transaction on vehicular technology, vol. 55, no. 4, pp. 1320-1330, 2006.
e. D.R.Stinson.Cryptography,TheoryandPractice.CRCPress,2000
f. Y. Liu, Y. Zhu, L. M. Ni, et al. "A reliability-oriented transmission serviceinwirelesssensornetworks,"IEEETransactionsonParalleland Distributed Systems, vol. 22, no. 12, pp. 2100-2107,2011.
g. G. X. Zhan, W. S. Shi, J. L. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197,2012.
h. M. Y. Hsieh, Y. M. Huang, H. C. Chao, "Adaptive security design with malicious node detection in

cluster-based sensor networks,"Computer
[5]. Communications, vol. 30, no. 1, pp. 2385-2400, 2007.
a. D.He,C.Chen,S.Chan,J.Bu,A.V.Vasilakos,"ReTrust:
[6]. Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, 2012.
a. F. Gómez Mármol, G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941.2012.
b. G. X. Zhan, W. S. Shi, J. L. Deng J L, "SensorTrust: A resilient trust modelforwirelesssensingsystems,"PervasiveandMobileComputing, vol. 7, no. 4, pp. 509-522,2012.
c. I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791- 802,2008.
d. S. Mandala, k. Jenni, M. A. Ngadi, et al. "Quantifying the severity of black hole attack in wireless mobile ad hoc networks." Security in Computing and Communications. Springer Berlin Heidelberg, 2014: 57-67.