A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks

Omid Naderi, Mahdi Shahedi, and Sayyed Majid Mazinani, *Member, IACSIT*

***Abstract*—As wireless sensor networks are characterized by severely constrained node resources, low communication range, low memory capacity and dynamic nature of WSNs, implementing security functionality and detection protocols to protect against *adversary* nodes becomes a challenging task. It is very likely that the encryption keys in the sensor nodes are accessed by attacker entities. The compromised nodes can launch sinkhole or wormhole attack to prevent the arrival of important information to the base station (BS). Establishing trust among distributed network entities has been recognized as a powerful tool to secure distributed networks such as MANETs and sensor networks. In this paper we first estimate the area in the network where a sinkhole attack has occurred there by considering the energy consumption model in the network. Then we present an entropy-based trust model in which more factors that affect trust computation are introduced. We apply a trust-based routing for providing a high level of security by path selection based on packet trust requirement. So it is needed that a routing protocol classifies the traffic packets according to their requested security and then routs the packets related to each class through the path that fulfills the security requirements of them. Our proposed approach that purposes to cover the mentioned problem is a resource efficient security protocol. This means that a trust value is allocated to the area suspected of sinkhole; the area is located by analyzing the energy of networks nodes and the packet is forwarded through low risk paths.**

***Index Terms*—Wireless sensor networks, sinkhole attack, trust model, secure routing.**

I. Introduction

In sinkhole attack the compromised node attracts the traffic of its neighbors by pretending that it has the shortest path to the base-station.and drops them. So it prevents the BS to receive sensed information completely and correctly. The sinkhole may launch a variety of attacks against the data traffic. If the sinkhole node drops the packets selectively we are facing a selective forwarding attack. Also it may modify some packets content and forwards them which is the most malicious type of sinkhole [1], [2]. Compromised nodes in selective forwarding attack are modeled as nodes that drop messages with probability p messages instead of forwarding them. When the probability p=1 we are facing sinkhole nodes [3]. In order to protect WSNs against malicious and selfish behavior, different secure routing protocols have been developed which mainly rely on cryptographic Basics and authentication mechanisms which are not suitable for WSNs. It is difficult to prevent packet dropping attacks by these manners because it is ambiguous whether the packet is dropped by an attacker or as a result of collision or noise. Trust management is a good solution for the above mentioned topics .We focus on a general event-driven communication model. In this paper we propose an approach to mitigate the impact of sinkholes in the network. In our approach we identify the area having the compromised node by employing a strategy of analyzing the energy of network nodes. A failure is detected if the consumed energy by one node (some nodes) has significant deviation from majority of network nodes .Then we introduce our trust measurement in which every node computed the trust value for its neighbors by using the direct trust value by itself and indirect trust values (or indirect observations which is also called recommendation trust). The trust mechanism will start after observing an energy consumption inconsistency in a network limited area and a trust value will be allocated to each nodes of this zone based on the required security by sensed event. Data are transferred through a path with relevant security and appropriate encryption. We present a secure and high delivery-ratio routing without tolerating the overhead caused by detection of compromised nodes. So it isn't necessary to waste the network energy for sinkhole nodes detection deterministically. In fact we develop a sinkhole resilient routing approach. The rest of the paper is organized as follows. Section II provides a brief overview of related work. In Section III we present a lightweight algorithm to detect the sinkhole attacked area. Section IV considers affected parameters by sinkhole attack and proposes a lightweight trust computation method and in Section V we design an optimized routing algorithm. Finally, in Section VI and Section VII we will provide the simulation results and some concluding remarks and outlines directions of future research.

Manuscript received April 3, 2014; revised June 13, 2014.

Omid Naderi and Mehdi Shahedi are with the Department of Computer, Science and Research Branch, Islamic Azad University, South Khorasan, Birjand, Iran (e-mail: omid_naderi85@yahoo.com, MhdShahedi@Gmail.com).

Sayyed majid Mazinani is with the Electrical Engineering Department, Imam Reza International University, Mashhad, Iran (e-mail: smajid_mizinani@yahoo.com).

II. Related Works

A. Sinkhole Solutions

1) Sinkhole detection approaches

In detection approaches a detection strategy is applied to detect the malicious node and remove it from routing process.

Ngai *et al*. [4] propose a lightweight algorithm to detect sinkhole attacks. In their approach the base-station collects the network flow information using a distributed approach, and then an identification algorithm analyzes the collected data to locate the sinkhole. Their work also considers a case in which there exist multiple colluded attackers in the network. Another intrusion detection system (IDS) for

detecting sinkhole attacks was presented in [5]. This system focuses on the Minot routing protocol that is based on link quality metrics to form a routing tree towards the base station. In each node, there is an IDS client which contains a cooperative detection engine, that stores two rules and monitors data to determine whether the traffic violets the rules. CPU usage of each sensor node in several time slots will be monitored in [6]. Appropriate functions f(x) are provided to describe the CPU usages patterns for network nodes under different scenarios (normal state and attacked state). Finally sinkhole detection problem is modeled as a problem of change-point of the CPU usage detection by using the provided functions.

2) Sinkhole prevention approaches

In this approach packet authentication is performed by applying an asymmetric encryption. Papadimitriou *et al.*, proposed a class of RESIST-h protocols, include of RESIST-0 and RESIST-1 that prevent malicious nodes from modifying their advertising distance to the sink more than h hops. The behaviors of malicious nodes of forging packets and hiding their ID's are prevented by this technique [7].

B. Trust in Sensor Networks

Due to the distributed nature of WSN, most of the existing trust management systems propose a distributed trust model which enables a subset of the nodes to evaluate the behavior of neighboring nodes and make decisions about them. The trust values are usually obtained taking into consideration different parameters such as personal reference (values obtained by first-hand interaction with the nodes, also known as direct trust) and reference (information obtained from non-personal interaction, also known as indirect trust) [8]. The proposed reputation-based trust model in WSNs by Chen *et al*. in [9], borrows tools from probability, statistics and mathematical analysis. They argued that the positive and/or negative outcomes for a certain event are not enough to make a decision in a WSN. They built up a reputation space and trust space in WSNs, and defined a transformation from the reputation space to the trust space [9]. Ref. [10] a Dynamic Trust Management System (DTMS) that counters two severe attacks (sinkhole and selective forwarding) on WSNs has presented. The trust is generated using equations that depend on simple successful and unsuccessful interactions between neighbors in a route. A node whose trust value falls below a threshold is not selected as next hop. Ref. [11], [12] discusses about the existing threats against a trust mechanism and limitations of watchdogs and considers issues about optimizing a determined threshold for better detection.

III. Sinkhole Area Detection Algorithm

In this section, we describe how to counteract a sinkhole attack without detection of the intruder .The proposed mechanism in this study utilizes the nodes energy and the energy deviation of each node rather than others in the same area to detect the zone suspected of having a sinkhole.

All detected suspicious nodes as well as nodes in their Neighborhood range are isolated as our work region. nodes energy information will be collected and analyzed by the sink .the nodes around the sinkhole deplete their energy faster than other nodes because the routes to the base-station that pass through sinkhole are used more frequently. Thus, an *energyhole* is formed around each sinkhole [13]. in other words since the compromised node pretends itself as the sink or a single hop count node to the sink, thus the *energy-sink-hole problem*(*hotspot*) also would be adapted to nodes near the compromised node. The *hotspot* problem implies that the sensors nearer the sink are responsible for forwarding data to it (on behalf of all other sensors in the network) suffer from a severe batter power depletion problem.

Ref. [14] we know it is also true for nodes nearer to compromised node (the malicious node forms a metaphorical sink) .So if we obtain the area with energy consumption model similar to energy model for the nodes near the sink, we can estimate an extremely small region which contains malicious node and its neighbors and detect the Approximate compromised node region by considering the energy Diagram. Since most often, the consumed energy by neighboring nodes of sinkhole is very similar to sinkhole node we only can identify the zone that sinkhole have occurred deterministically not the compromised node. The average energy consumption of a node located near the sink is modeled in [14] which can be extended the nodes near the hole node.

We focus on the source sensors within a distance $r \le \sigma \le R$ from the sink, where R stands for the radius of the communication range of the source sensors.

More specifically, we consider a circle c_σ of radius σ around the sink *s*, c_σ includes the source sensors that forwards data on behalf of all other source sensors to s, *D* is the radius of the circular deployment field C_D that is outside c_σ .Using the energy model presented in [14] the energy consumption per source sensor using the base protocol is given by:

$$E(C_\sigma) = \varepsilon\left(\frac{2}{\alpha+2} + \left(\frac{2}{3}\right)^{\alpha}\right)\sigma^{\alpha} + \left(\frac{2D^2}{\sigma^2} - 1\right)E_{elec} \quad (1)$$

It is assume that the energy consumption of the sensors is due to data reception, transmission for static sink network. where $E_{elec} = 50 \times 10^{-9}$ is the electronics energy, ε is the transmitter amplifier ($\varepsilon = 10^{-11}$ for $a = 2$ and $\varepsilon = 13 \times 10^{-16}$ for $a >= 3$),and a is the path-loss Exponent ($2 <= a <= 4$) .

Fig. 1 in [14] shows that $E(c_\sigma)$ increases significantly as the distance becomes shorter to the location of the sink (sinkhole).

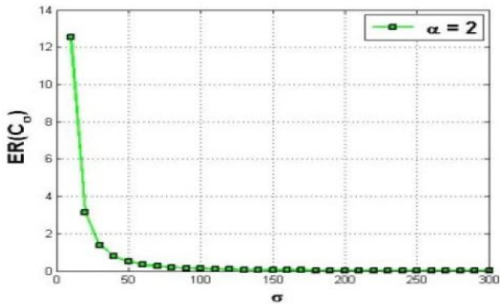

Fig. 1. Plot of $E(c_\sigma)$.

In fact if there is a node which as we come nearer it, the

network consumed energy of the network is increased Exponential it will be the interested node (sinkhole node makes an energy hole around itself) .So if sink collects the consumed energy pattern of network nodes in a few time slots, it can detect the nodes that their energy is corresponding to $E(c_{\acute{o}})$ and finally estimates the malicious node area .In other word we can easily compute energy deviation of each node from the average energy consumption of the source sensors.

If E_1 , E_2,...., E_i stand for consumed energy after several slots in *network* f ($E_{\text{deviation}}$) computes the deviation from average :

$$f(E_{\text{deviation}}) = \left(E_i - \overline{E}\right)^2 \quad (2)$$

The average consumption energy of two zones in the network have illustrated in Fig. 2 after multiple time slots. After calculating f functions for all network nodes, this zone is estimated as the sinkhole attacked zone and a comparison have performed with a free attacked zone in the network. Both zones have the same radios.

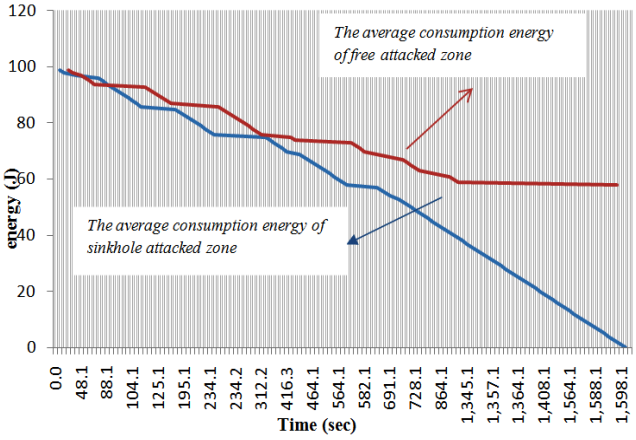

Fig. 2. Energy lost process in different zones.

As we see in Fig. 2 the energy lost process is similar for both zones up to nearly second 400s but after that the attacked area starts to deploy the energy dramatically while the safe zone decreases the energy smoothly.

For each node that f function value is more than a predefined threshold it is the suspicious node.

As it is mentioned a trust allocation mechanism is enabled in the work area in second step. While the energy consideration leads to estimate the area that a sinkhole is occurring, watchdogs in each sensor in the area starts observing its neighbors. Thus the nodes aren't always monitoring their neighbors and it causes to save the power and the memory.

To prevent the modifying message by malicious nodes the packets are encrypted in the symmetric cryptography RC5 algorithm.

IV. Proposed Trust Mechanism

A. Node Behavior Monitoring

it is assumed each sensor node has a watchdog which monitors and records one hop count neighbor's behavior such as transmition [12], in Fig. 3 when A forwards a packet to B, the watchdog in A can overhear B's forwarding and then verify whether the packet is forwarded by B or not by using the sensor's overhearing ability within its transceiver range.

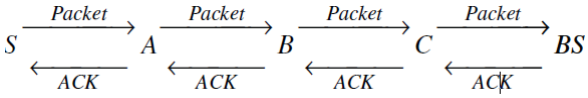

Fig. 3. A routing path having three intermediate nodes A, B, and C.

B. Trust Computation of Nodes

The concept of trust describes the certainty of whether the agent will perform an action in the subject's point of view. Let T {subject: agent, action} denote the trust value of the Relationship {subject: agent, action} [15]. For example the number of successful forwarded messages from A to B divided to the total transmitted messages [11] can be a suitable metric for packet dropping attack but it can't covers all the characteristics of sinkhole and selective forwarding attacks .this trust value is the Beta trust model:

$$T\{\text{subject: agent, action}\} = \frac{S+1}{N+2} \quad (3)$$

If an observed node forwards the packet s times and drops f time among the total N packets . ($N = s + f$, $0 <= T <= 1$)

Another presented trust value is entropy trust model [15]:

$$T\{\text{subject: agent, action}\} = \begin{pmatrix} 1 - H(p) & for\ 0.5 \le p \le 1 \\ H(p) - 1 & for\ 0.5 \le p \le 1 \end{pmatrix} \quad (4)$$

We proposed entropy based trust model and try to regard to the sinkhole specification in it. Before the describing our trust model we discuss about how to determine suitable threshold. if we determine trust threshold very low, there will be a high false alarm and if a high trust threshold is determined it needs to pass a long time from dropping packets by the compromised node to detect it [10]. We consider two types of traffics: high-security-demanded traffic (HSD traffic), normal- security-demanded traffic (NSD traffic) the classification is intended in terms of the security quantity which should be provided for each type of traffic. In here, we employ two different threshold as a solution for the mentioned issues, θ_h , θ_n . If the trust level of a node comes blow θ_h , this node cannot use for forwarding the HSD packets and only will be able to rout the packet with Requested normal security level, if the trust level of a node also goes blow θ_n , the node can't even use for routing normal demanded security packets .

In addition in situations where a suitable node can't be find in the network to forward HSD packets and if the network stability Maintaining and continuing forwarding packets is important for us, the determined threshold would decrease as much as the node trust value with highest trust level in the network.. In fact the specified threshold for routing packets can change in special conditions dynamically. In sinkhole attack, the attacker after certain number of initial successful forwarding (to build a high trust value), can drop a considerable number of packets consecutively without bringing its trustworthiness below the threshold [8]. In this case the trust value of node comes down significantly but it

won't fall below the threshold because of the intelligent estimation of attacker, and can reach to Primary trust level after enough number of forwarding. The amount of distance of malicious node to sink can affect on the amount of vulnerability in the network. As a rule of thumb, whatever the malicious nodes are closer to the sink; more packets are prevented to arrive. Thus the trust value allocated to a suspicious node (a suspected node to sink hole) near the sink should be lower compared to the case the node is Farther the sink. In other words, for the nodes near the sink malicious and selfish behaviors have a more effect on the trust values and the node must do long-term good behaviors to build up a good reputation, only a few bad actions can ruin a reputation.

This logical relation is shown in Fig. 4. We show in Fig. 4 how *d* (stands for distance from current low trust node to sink) have effect on the maximum packet drop rate (MPDR) defined in [4740a134] as the metric.

$$MPDR\ (\%) = (N_D / N_R) \times 100 \tag{5}$$

where *ND* is the total number of dropped packets and *NR* is the total number of received packets

So the beta-trust model after some manipulation we get :

$$T = \frac{S+1}{S+F+2} \times \frac{h_{curr}}{h_{\max}} \times \gamma (0 \le T \le 1) \tag{6}$$

h_{max} is the Hops from the farthest node to BS and h_{curr} represents the distance from the current node to sink. γ ($0 \le \gamma \le 1$) is a weighed parameter which can obtain different values from the evaluating neighbor node base on the evaluated malicious node alternative behavior. If a node has dramatic alternative behavior patterns (behave well and badly alternatively) γ gets smaller values from the neighbor nodes and causes a small trust value. In contract, if the node has a good and confident behavior γ is set in a way that the short distance to sink doesn't decrease the trust value of the node.

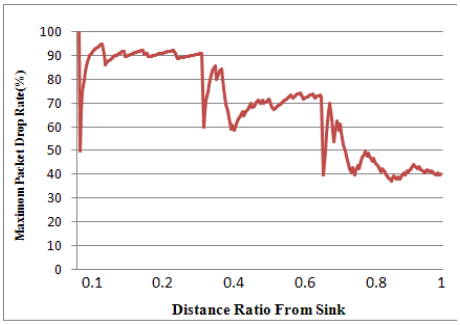

Fig. 4. MPDR of low trust nodes as distance increases.

As an example when the attacker estimates the threshold for HSD packets, it drops the packets in a way that the trust value stays near the threshold but doesn't fall below it, if this node is placed in the sink neighborhood its trust value comes down significantly rather than other nodes and only can forwards the NSD packets.

We can also show that different distributions of suspicious nodes (low trust value nodes) in the network, specially around the sink have effect on the amount of vulnerability in the network .we define *dis* as the distribution pattern of the suspicious nodes and show how *dis* have effect on MPDR .*dis* is a quantitative parameter that can get different values depending on the amount of vulnerability produced in the network by different distributions of compromised nodes. We determined $0 \le dis \le 1$ and *dis* parameter that is given by the sink can be specified base on distribution pattern statically.

We consider three distributions (see the Fig. 5):

Normal distribution, with center of the sink and σ^2 as the variance of the distribution.

Ring distribution, the compromised nodes form a ring of nodes around the sink.

Linear distribution, the compromised nodes form a line from sink in to the network.

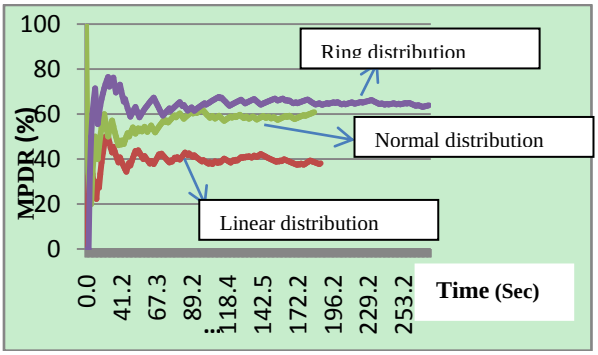

Fig. 5. MPDR of different low trust nodes distribution.

Sink identify all the nodes in the transmission range with low trust level which are extremely near the threshold but not under the threshold (suspected nodes).

So The improved beta trust goes in the fallowing form:

$$T = \frac{S+1}{S+F+2} \times \frac{h_{curr}}{h_{\max}} \gamma \times dis \tag{7}$$

The final our entropy based trust model will be:

$$T_{i,j} = \alpha \times DT_{i,j} + \beta \times IDT_{i,j} \tag{8}$$

Including $\alpha + \beta = 1, \alpha > 0, \beta > 0$, $DT_{i,j}$ represents the trust value that node i compute for node j in direct interaction. $IDT_{i,j}$ is the indirect trust value that node i calculates for node j by the nodes in its neighboring range . In fact $IDT_{i,j}$ shows the trust relations between distributed nodes without direct interactions by its neighbors. The following represents the indirect trust evaluation process:

$$IDT_{i,j} = \sum_{k \ne i, k \ne j, k \in c_j}^{n} DT_{i,k} \times DT_{k,j} \Big/ \sum_{k \ne i, k \ne j}^{n} DT_{i,k} \tag{9}$$

$IDT_{i,j}$ Stands for the recommendations provided by node which belongs to the neighbor set *Cj* of node *j*. *n* denotes the number of neighbors.α and β are weighed factors which are associated with the security policies. A larger value for α indicates that the sensor node in WSNs is more convinced

about its own judgment. Similarly, a larger value for β means that the recommendations provided by other nodes are more trustworthy in trust evaluation process. In addition, the trust value is subject to $-1 \leq T_{i,j} \leq 1$ ([16]).

V. Differentiated Route Establishment and Data Forwarding

We provide a routing approach to increase security. We present a routing protocol with different secure paths which utilizes the computed trust values as a parameter to establish routes. The proposed protocol is base on the presented protocol in [17] for delay sensitive data. The routing process starts by the sink. Sink sends request packet when the user needs some information or get a report periodically and collects the related data *(request diffusion stage)*.

After the request diffusion every sensor which had sensed the interested event will report it to the sink by a report packet .The report must have the information related to the occurring event and the security level that it needs however basic data related to the event are sent in the data forwarding stage . a temporary routing table is created in this stage. The event packet broadcasts in the network. Each node receives the packet forwards it to its neighbors and it is repeated until receiving packet by the sink. Each intermediate node which receives the packet creates a record and inserts it into routing table, The trust value of the path up to current node, the source node id, the sender node id, and the number of covered hops are kept in this record. The trust value of the path up to current node, is the minimum trust of nodes up to here (the most trusted path is the path with highest minimum trust). In this routing table is determined all the possible routes by considering the trust values of the paths between the sink and the source node sensing the event (*event occurrence message stage*).

Final when a confirmation packet is sent to the source node by the sink which informs it is ready to receive data from source, simultaneously forwarding the packet from sink; forwarding paths with different trust levels are created. to construct different trust level paths, the temporary routing table is sorted based on trust value column for each node id (the column values show trust value of a path from source up to this node id) .therefore the first record (records) related to each node ID represent the least risk path up to this node .and the constructed path by these first records is used for high-demanded security traffic (most trustable path).the last records are used in routing normal security traffics. The path with the minimum trust value that is equal or greater than the determined threshold will be selected for the sensed event. If there isn't such a path the confirmation packet is dropped in a rerouting process and sink forwards another packet to source for route establishment but in this time the determined threshold for the event decreases to the highest existence trust value in the network. In fact the chosen threshold will be changed dynamically base on the network conditions. We have applied the symmetric RC5 algorithm [18] to prevent the content modification by low trust nodes .RC5 present a flexible encryption structure and the user can easily manipulate the parameters to obtain a tradeoff between higher speed and higher Security. We have encrypted the HSD packets with a more number of rounds which causes more security. RC5 32/32/16 was applied for the HSD packets and NSD packets were encrypted by RC5 32/12/16. (Rout establishment and data forwarding stage).

VI. Performance Evaluation

In this section, the OPNET modeler simulator is used to evaluate the performance of our proposed trust based design against sinkhole attacks .we evaluate the presented approach effectiveness against sinkhole attack and selective forwarding , and the gain resilience to packet dropping by the malicious nodes in our adaptive trust protocol have compared to resist-0 protocol in [3]. We consider an event driven network model which each sensor periodically sends data to sink or data is sent to sink base on the sink request. The malicious nodes can launch grayhole and blackhole so they drop every received packets with probability p=1 or less respectively the compromised node try to attract more traffic by advertising a shorter distance to sink. Our simulations model a network consisting of 100 sensor nodes placed randomly within a 200m × 200m area. We define two types of sensor nodes in the simulations: well-behaved nodes and malicious nodes

The initial trust is set to 0 for every node in the network. We perform our implementation base on the presented metric in [3] which names Risk Factor .it is an evaluation metric and in the case we know the malicious node we can calculate the risk of entire topology by this metric. The risk factor for each node *X* shows the probability that a message from a node X arrives at a compromised node on its way to sink.

In the simulation, we increase risk of the network and destroy it more and more as the risk factor is increased gradually to evaluate the protocol performance in different situations. A great value of risk factor means the more compromised nodes and their short distance to sink.

A. Evaluation of the Trust Based Protocol

We consider the case that the malicious nodes in the network can launch *blackhole* and *grayhole* attacks, then obtain the packet delivery rate to the sink in the network (see Fig. 6).

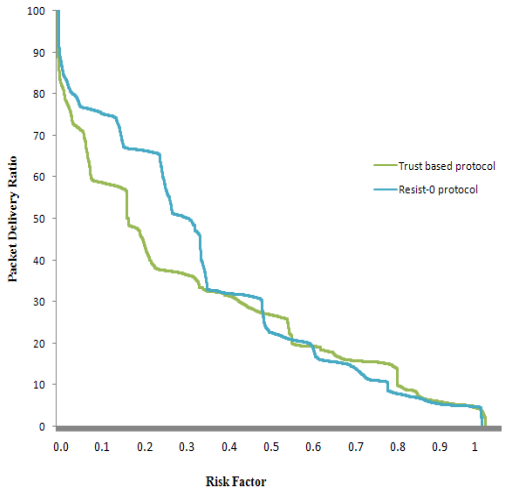

Fig. 6. Performance of trust based protocol and resist-0 under the sinkhole attack.

The result shows Resist-0 can perform better than the trust based protocol in low risk factors. In low risk(low malicious

sensor nodes and low number of packet dropping) it is difficult for the proposed protocol to identify the area which the sinkhole has launched and takes more time since the protocol locates the sinkhole area base on an energy inconsistency. So our approach achieves significant performance in higher risk factors and be able to deliver more packets to sink in hard conditions since in this case malicious nodes have exponential energy depletion and the suspicious area is easy to be estimated.

But resist-0 performs completely different, it prevents to malicious nodes lie about their authentication and their distance to sink base on the routing protocol. So the compromised nodes can't attract high volume traffic from beginning of work.

B. *Effect of Designing Multipath Routing on the Proposed Approach*

If we apply multi-path routing to forward packets to sink, a better improvement will be obtained for the trust based protocol rather than the resist-0 in single path routing (Fig. 7). The routing should perform through the candidate paths with a trust value which provide the required security of the traffic. A packet is sent from two paths to the sink with trust values equal or greater than the interested threshold .multipath routing decreases selective forwarding attacks significantly.

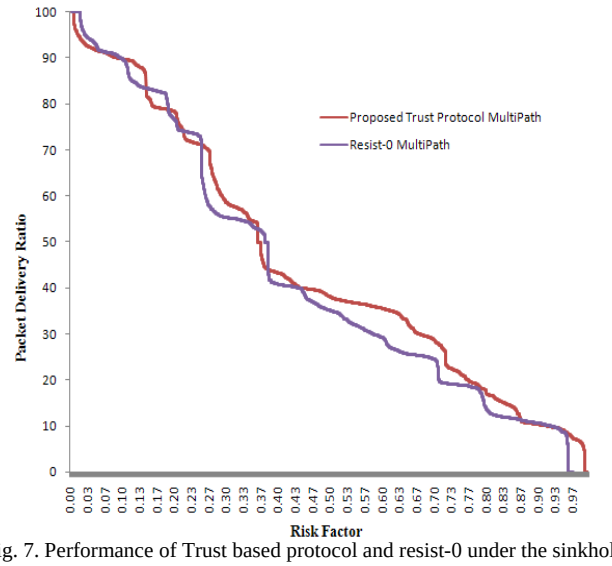

Fig. 7. Performance of Trust based protocol and resist-0 under the sinkhole attack using two paths for routing.

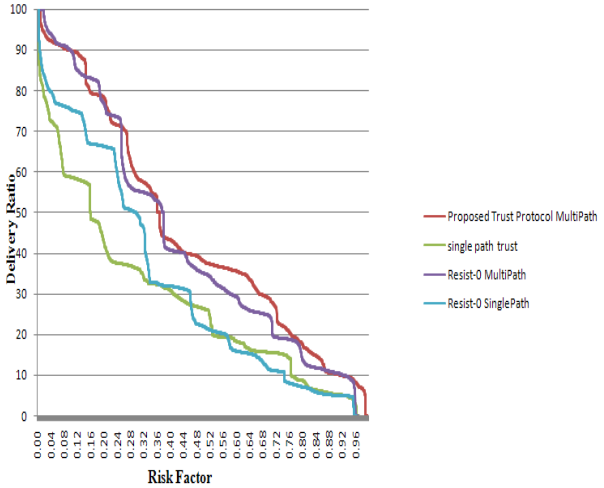

Fig. 8. Comparison of the proposed protocol and resist-0 in two cases: single path and multipath routing.

In Fig. 8 we have compared packet delivery rate in two case of single-path and multi-path routing. We clearly observe the gained improvement in received data by the sink in multi-path routing.

VII. Conclusion

In this paper we have presented an efficient algorithm to mitigate the effects of sinkhole attacks. In the presented approach, firstly the area which has been attacked by the attacker is estimated by energy consideration of nodes. We also define a trust relation that addresses the sinkhole specification better. Our approach utilizes an adaptive routing protocol to deliver the packets to the sink.

References

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, 2003, pp. 293-315.

[2] T. Chanatip and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," in *Proc. 7th International Conference on Information, Communications and Signal* IEEE, 2009, pp. 1-5.

[3] L. Fessant *et al.*, "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis," *Computer Communications*, vol. 35, no. 2, 2012, pp. 234-248.

[4] E. Ngai, J. Liu, and M. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11, pp. 2353–2364, 2007.

[5] K. Ioannis *et al.*, "Intrusion detection of sinkhole attacks in wireless sensor networks," *Algorithmic Aspects of Wireless Sensor Networks*, pp. 150-161, Springer Berlin Heidelberg, 2008.

[6] C.-L. Chen, M. Song, and G. Hsieh, "Intrusion detection of sinkhole attacks in large-scale wireless sensor networks," in *Proc. 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, pp. 711-716, IEEE, 2010.

[7] J. A. Chaudhry *et al.*, "Sinkhole vulnerabilities in wireless sensor networks," *International Journal of Security & Its Applications*, vol. 8, no. 1, 2014.

[8] L. Javier, R. Roman, I. Agudo, and C. F. Gago, "Trust management systems for wireless sensor networks: Best practices," *Computer Communications*, vol. 33, no. 9, pp. 1086-1093, 2010.

[9] H. Chen, H. Wu, X. Zhou, and C. Gao, "Reputation-based Trust in wireless sensor networks," presented at International Conference on Multimedia and Ubiquitous Engineering (MUE '07), Seoul, Korea, 2007.

[10] N. C. Debnath *et al.*, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," in *Proc. IEEE Symposium on Computers and Communications*, pp. 537-542. IEEE, 2008.

[11] L. Sun *et al.*, "Defense of trust management vulnerabilities in distributed networks," *Communications Magazine, IEEE*, vol. 46, no. 2, pp. 112-119, 2008.

[12] Y. Cho *et al.*, "Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks," in *Proc. 2012 IEEE Symposium on Security and Privacy Workshops (SPW)*, pp. 134-141, IEEE, 2012.

[13] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644-653, 2014.

[14] H. Ammari, "Investigating the energy sink-hole problem in connected k-covered wireless sensor networks," vol. 1, no. 1, 2013.

[15] L. Sun *et al.*, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305-317, 2006.

[16] J. Q. Duan, D. Yang, H. Q. Zhu, S. D. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, 2014.

[17] A. Rezaee *et al.*, "HOCA: Healthcare aware optimized congestion avoidance and control protocol for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 37, pp. 216-228, 2014.

[18] Rivest and L. Ronald, "The RC5 encryption algorithm," *Fast Software Encryption*, pp. 86-96, Springer Berlin Heidelberg, 1995.

Omid Naderi was born in 1988 in Mashhad, Iran. He received his BS in computer engineering from Islamic Azad University of Mashhad (IAUM) in 2010 and he is a master of computer software engineering student at Islamic Azad University of Birjand (IAUBir). His research interests are security providing in wireless sensor networks, computer networks and quality of service.

Mehdi Shahedi received the BA degree between 2007-2011 in computer software engineering from Islamic Azad University of Mashhad, Iran, the MS degree in computer software engineering from Department of Computer, Science and Research branch, Islamic Azad University, South Khorasan, Birjand, Iran between 2012-2014. From 2010, he is net and oracle developer and project manager in HRM Project in DadeGostar Toos Co. His main research area is computer networking, include mobile sink routing protocol for delay sensitive traffic in wireless sensor network and image processing.

Sayyed Majid Mazinani was born in Mashhad, Iran on January 28, 1971. He received his bachelor degree in electronics from Ferdowsi University, Mashhad, Iran in 1994 and his master degree in remote sensing and image processing from Tarbiat Modarres University, Tehran, Iran in 1997. He worked in IRIB from 1999 to 2004. He also received his Ph.D in wireless sensor networks from Ferdowsi University, Mashhad, Iran in 2009. He is currently an assistant professor at the Faculty of Engineering in Imam Reza University, Mashhad, Iran. He was the head of the Department of Electrical and Computer Engineering from 2009 to 2012. His research interests include computer networks, wireless sensor networks and smart grids.