Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 326295, 9 pages
http://dx.doi.org/10.1155/2013/326295

Research Article

Secure Ant-Based Routing Protocol for Wireless Sensor Network

Nabil Ali Alrajeh, Mohamad Souheil Alabed, and Mohamed Shaaban Elwahiby

Biomedical Technology Department College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 25 May 2013; Accepted 16 June 2013

Academic Editor: S. Khan

Optimal path selection in wireless sensor networks (WSNs) is one of the challenging tasks. Several efficient routing protocols are proposed for specific scenarios to achieve particular objectives in WSN. However, such networks have many limitations such as low data rates and security threats. In this paper, we propose an adaptive secure routing protocol which is based on bioinspired mechanism. It uses distributed ant-based methodology to select two optimal paths keeping in view route security. Simulation results show that our routing protocol can perform better in many scenarios.

1. Introduction

WSNs are usually deployed in such areas where other wired and wireless networks are not feasible to be established and configured. It consists of low power sensor nodes and high power sink and is typically used for environmental monitoring. Sensor networks normally operate in decentralized and distributed manner in which sensor nodes have the capability of self-healing and self-configuration. Due to physical hostile environment and multihop and distributed architecture, WSN is more vulnerable to different types of security attacks. An attacker can easily launch security attacks against physical, media access, or network layer to WSN.

Security is one of the most important aspects in deploying or designing a sensor network. As WSN is deployed in harsh and extreme environment, it is not possible to protect it from security attacks by physical monitoring.

Most applications of WSN need security considerations especially military-based applications and monitoring. Sensor nodes are of low cost and small in size due to which heaving security mechanisms cannot be used. The reason is that heavy security mechanisms demand more processing power, more memory, and more battery resources which may increase the cost. Furthermore, most of sensor nodes are not tamper resistant, and the attacker can extract the sensitive data from the nodes and even configure few nodes for malicious activities and false data routing from source to destination.

Secure routing is one of the optimal solutions to counter network layer security attacks. In WSN, the data is more vulnerable to different security attacks during data transmission from source to multihop away destination [1, 2]. This is the reason; secure routing is always desirable in such kind of networks.

An attacker can conduct variety of security attacks against WSN, such as blackhole, greyhole, sinkhole, false routing updates, packet modification attack, packet misdirecting attack, and hello flood attack [3–7]. These security attacks bring serious routing malfunctions in data transmission from source to destination. Some attacks are less severe while some have more severity. For example, greyhole attack selectively forwards packets to the next hop, whereas blackhole and sinkhole attacks drop all the packets and create a denial of service (DoS) situation. These network layer security attacks can be prevented by appropriate secure routing protocol.

Secure routing is an important step for designing and deploying multihop wireless networks such as WSN. Multihop wireless networks are more vulnerable to security attacks as compared to single-hop wireless networks. The reason is that most of multihop wireless networks are distributed having no centralized body. Designing an appropriate secure routing protocol for WSN is a challenging task. In WSN the ideal routing protocol should be secure and efficient in terms of data delivery, route discovery, and routing overheads.

Research community has proposed many methodologies for designing secure routing protocols. Few important

methodologies are cross-layered mechanisms, multipath mechanisms, and bioinspired mechanisms.

In cross-layer mechanism, parameters are exchanged across different layers of protocol suit for optimal path selection from source to destination [8, 9]. However, this methodology requires more computation, memory, and battery resources. The advantage of this methodology is its capability to counter multilayer security threats. In multipath mechanism, two or more paths are established from source to destination [10, 11]. The data is routed through many paths instead of one, and therefore such mechanisms are considered more fault tolerant as compared to single path. Bioinspired mechanisms are considered more robust as they provide interesting solution for routing due to their inherent scalable features [12].

In this paper, we present an adaptive secure routing protocol which is based on bioinspired technique termed as ant colonization. Our protocol has three important features which are listed as follows.

(i) *Adaptive Security Nature*. The proposed protocol provides adaptive security mechanism.

(ii) *Two Paths Selection*. The proposed routing mechanism selects two paths for data transmission. The proposed mechanism ensures security of both routes.

(iii) *Bioinspired Technique*. The proposed routing algorithm is based on ant colony optimization (ACO) technique.

Our proposal is able to select optimal paths from source to destination by ensuring adaptability, robustness, and security. The rest of the paper is organized as follows. Section 2 discusses related work. Protocol design considerations are covered in Section 3. Section 4 describes the evaluation and simulation results. Section 5 concludes the paper.

2. Related Work

WSNs have many real-life applications such as military applications, healthcare applications, forest and habitat monitoring, fire, heat, and pressure monitoring in a given area [13]. Selection and delivery of data packets from source to destination is one of the important tasks in WSN. Researchers have proposed many routing mechanisms so far [14–18]. However, majority of WSN routing protocols are application dependent without any consideration for security aspect. Security concern is gaining significant attention and many secure mechanisms have been proposed for WSN [19–23]. However, many of these security mechanisms operate at different layers to counter specific risk situation. To counter network layer security attacks, secure routing is more appropriate security mechanism. In last few years, variety of secure routing protocols are proposed for sensor networks [24–27].

In WSN, base station periodically broadcasts the routing information. The attacker can easily misdirect, drop, or modify the data during transit. A security mechanism termed as μTesla [28] is used to protect base station broadcast data from modifications. μTesla uses symmetric cryptography which provides authenticated broadcast. This scheme is expensive due to long one way hash chain. An authenticated routing message in sensor network (ARMS) [29] is proposed to overcome shortcomings of μTesla. It uses shared secret key and one way short hash chain. Enhancement of fault tolerant ad hoc on-demand distance vector (ENFAT-AODV) [30] is proposed to address the issue of node failure. A backup path is established which is used whenever the main route is not available due to node failure. Sensor nodes are deployed in distributed manner, so trusted neighbor discovery is an important task. Cross-layer secure routing protocol using energy harvesting mechanism in wireless sensor networks is proposed in [31]. Secure alternate path routing in sensor network (SeRINS) uses key management scheme along with neighbor report system [32]. The objective of this mechanism is to protect WSN from attacks such as packet modification or bogus routing information. Another secure approach that uses secret key cryptography with rekeying support is proposed for WSN [33].

As we know WSNs have resource constraints in terms of data rates, battery power, computation, and memory, and therefore it is highly desirable to design and propose such security mechanisms especially routing protocols which are light weighted so that the critical resources are reserved and to enable sensor nodes for long-time operations. Secret keys sharing and management requires more resources. Bioinspired mechanisms offer robust, fast, and inexpensive solutions for securing WSN. Ant colony optimization (ACO) is one of the bioinspired techniques, which provides robust and interesting solutions for WSN routing protocols.

Termite algorithm is inspired from the termite colonies [34]. Termite is a hybrid protocol in which route is discovered on demand by the ants while the data packets implicitly maintain the quality of paths in proactive manner. In this approach forward ants unicast and follow a random path while backward ants may or may not use the same path. Optimized termite [35] uses the concept of termite with the objective of enhancing load balancing mechanism. This algorithm selects such a route having less traffic. Ant-dymo [36] is basically proposed for ad hoc networks, and it is based on ACO. Ant-dymo aims to improve the end to end delay and packet loss. This algorithm uses two types of artificial ants, explorer ant, which explores the route in proactive manner, and search ant responsible for searching for specific destination in case it is not present in the routing table. AntHocNet [37] sends reactive forward ants for route discovery between source and destination and proactive forward ants are used to test the quality of existing paths and explore alternate best paths. AntOR [38] is based on Ant Colony Optimization with some modifications in AntHocNet routing algorithm. AntOR provides better load balancing by satisfying multiple quality of services constraints and lower control overhead by imposing some restriction on the exchange of routing information. GrAnt [39] is a prediction-based routing algorithm which provides higher packet delivery with low routing overhead. GrAnt depends on both local information and global information. In [40], ant-based framework for routing in WSN along with mathematical theory of bioinspired computation is presented. An energy efficient ant-colonization-based routing algorithm is proposed in [41]. In this algorithm,

Table 1: Different stages of proposed protocol.

Stage	Operation
Route discovery	Initial discovery of two or more routes
Route selection	Selection of appropriate routes
Security	Implementation of security mechanism
Data forwarding	Forwarding of data from source to destination

each individual packet is treated as an ant, which communicates with others through pheromone. Each sensor node maintains a table known as pheromone table. Biologically inspired optimization for sensor lifetime (Bio4sel) [42] is a decentralized, autonomic, and distributed ant-based routing algorithm that aims to increase sensor network lifetime. Another energy efficient routing protocol is presented in [43]. This scheme uses dynamic route identification scheme in case of path failure due to dead node or intrusion. The objective of this routing protocol is energy efficiency and path reliability.

Most of the bioinspired routing protocols based on ant optimization technique are efficient in terms of optimal path selections. ACO-based routing protocols are less expensive in terms of battery, computations, and memory usage; however, they cannot perform well in case of security attacks due to lack of security mechanism. As we know, WSNs are deployed in harsh and hostile environment, and therefore some sort of security mechanism is indeed necessary along with bioinspired methodology.

3. Proposed Routing Scheme

WSN is gaining more attention due to its wide range of usage and applications. Security consideration is one of the important factors as most of WSNs are deployed in harsh and hostile environment. That is why secure routing is highly desirable for transmitting data from source to destination. The proposed mechanism is secure routing based on ant colony optimization (ACO) technique.

The proposed routing protocol consists of four stages which are listed as follows:

(i) route discovery;

(ii) route selection;

(iii) route security;

(iv) data forwarding.

The proposed scheme is presented in Table 1.

Ants are able to select the shortest path from source to destination, that is, from home to a food. Ants drop a chemical substance termed as pheromone along the path. Generally, shortest path has more intensity and concentration of pheromone as compared to other paths. There are two important categories of ants; one is forward ants and the second is backward ants. In our scheme we utilize this scheme for route request and route reply mechanisms.

Before route discovery process, the proposed routing protocol uses simple mechanism to discover surrounding neighbors using hello packets. The routing table is updated on the basis of responses received from surrounding neighbors. During route discovery process, source node broadcasts a fixed number of ants (route request packets (RREQ)) to random neighbors. The source node also sets a lifetime interval of RREQ ants. These RREQ ants are acting as forward ants. Forward ants travel through intermediate nodes and find destination (food). The destination receives many RREQ ants through random intermediate nodes. However, total numbers of RREQ ants received at destination are equal to or less than that sent by source node, as some of the RREQ ants may not reach to destination due to congestion, expiration of lifetime interval, or path failure. The destination node sends back route reply (RREP) ants using the same paths which are used by forward ants. RREP ants act as backward ant. The packet formats of forward and backward ants are almost same; however, backward ant has a field *path_security*, instead of *reputation_value*. Path security field accepts only two values; that is, 1 or 0. 0 means that the path is not secure and needs security mechanism while 1 means that the path is secure and there is no need to enable security mechanism.

Table 2: Packet format of forward ant.

Field	Description
S_ID	Source ID of originating node
D_ID	Destination ID
H_count	Hop count from source to destination
Lifetime	Lifetime of packet
Reputation_value	Trust and reputation value of next neighbor

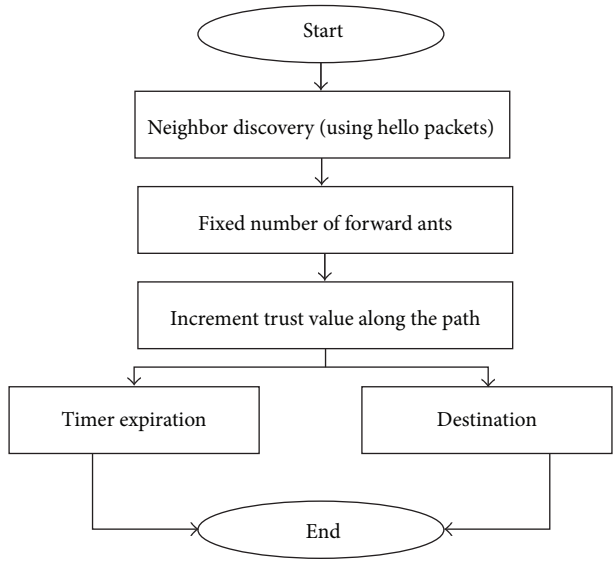

Figure 1: Forward ant process.

The packet format of forward ant is given in Table 2.

The algorithm for forward ant process is presented in Figure 1.

The algorithm for backward ant process is presented in Figure 2.

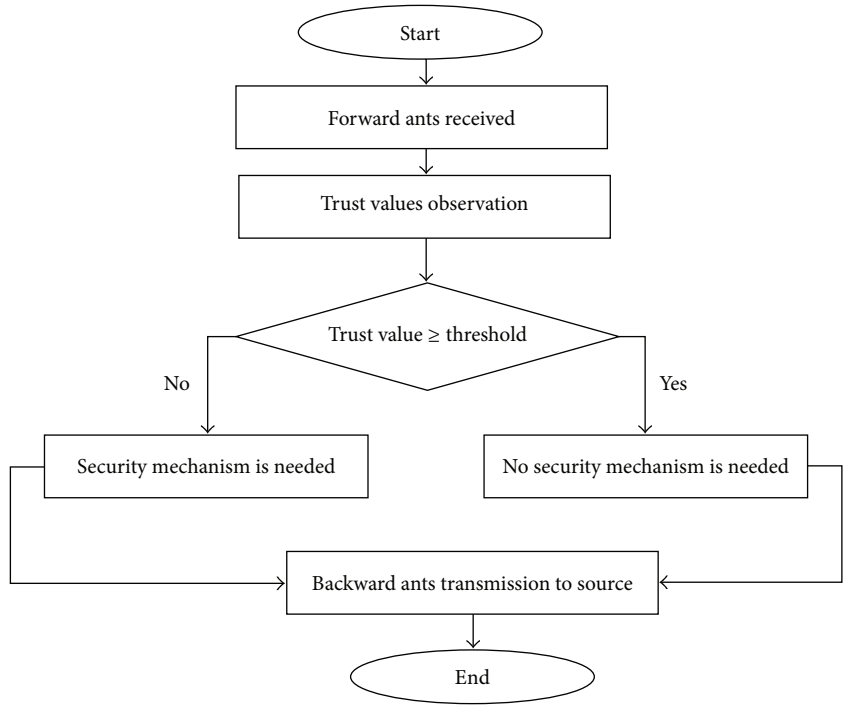

Figure 2: Backward ant process.

The route discovery processes have two important features.

(i) Propagation of fixed numbers of forward ants, which are responsible to increment reputation value along multihop path till destination, is clear.

(ii) Destination node receives random numbers of forward ants and responds using backward ant propagation towards source node. The destination node enables *path_security* field to specify whether the source node needs to ensure security or not by observing reputation values.

When source node receives many backward ants RREPs packets, then route selection procedure is triggered. In route selection process, source node examines all the received backward ants and chooses two paths considering security features. The route selection process is presented in Figure 3.

The route discovery and route selection process of proposed mechanisms is inspired from ACO [44]. Suppose that there are four ants (A1, A2, A3, and A4) and four different routes (R1, R2, R3, and R4) are available to food (F). The four ants at the starting point (S1) have no knowledge of the food.

(i) Ant A1 selects route R1. Similarly ants A2, A3, and A4 select routes R2, R3, and R4, respectively.

(ii) A1, A2, A3, and A4 randomly reach food (F).

(iii) Suppose that Ant A3 faces less hurdles along the path, so it left high concentration of pheromone. It means that the trust value of R3 is greater as compared to other routes.

(iv) At destination, the trust values of all paths are computed.

(v) From destination, all four ants followed their own path toward the starting point.

(vi) At starting point, two paths are now selected on the basis of path_security value.

(vii) Now the ants travel using those two paths which are more secure.

The security mechanism in proposed routing protocol is based on watchdog mechanism [45]. In our scheme, watchdog is implemented on every sensor node. Sensor nodes monitor all surrounding neighbors in their radio range using watchdog. On the basis of the mutual monitoring mechanisms, node can classify its neighbors as cooperative or noncooperative. Watchdog mechanism is capable to monitor neighbors, collects data, and observe data forwarding behavior of surrounding nodes. In our approach, a reputation value is assigned to all neighbors, and whenever a forward ant arrives, the reputation value of next neighbor is incremented.

The destination node (sink) makes the decision by enabling 0 or 1 in the backward ant propagation whether source node needs to send encrypted data or not. When source node receives the backward ant having 0 in the path_security field, an encryption mechanism is used to ensure data security. We are using lightweight encryption mechanism which is discussed in [46]. In this mechanism, permutated key is generated by RC4. The key to RC4 encryption changes dynamically, and thus every data packet has a different dynamically generated key.

The complete working mechanism of proposed routing protocol is presented in Figure 4.

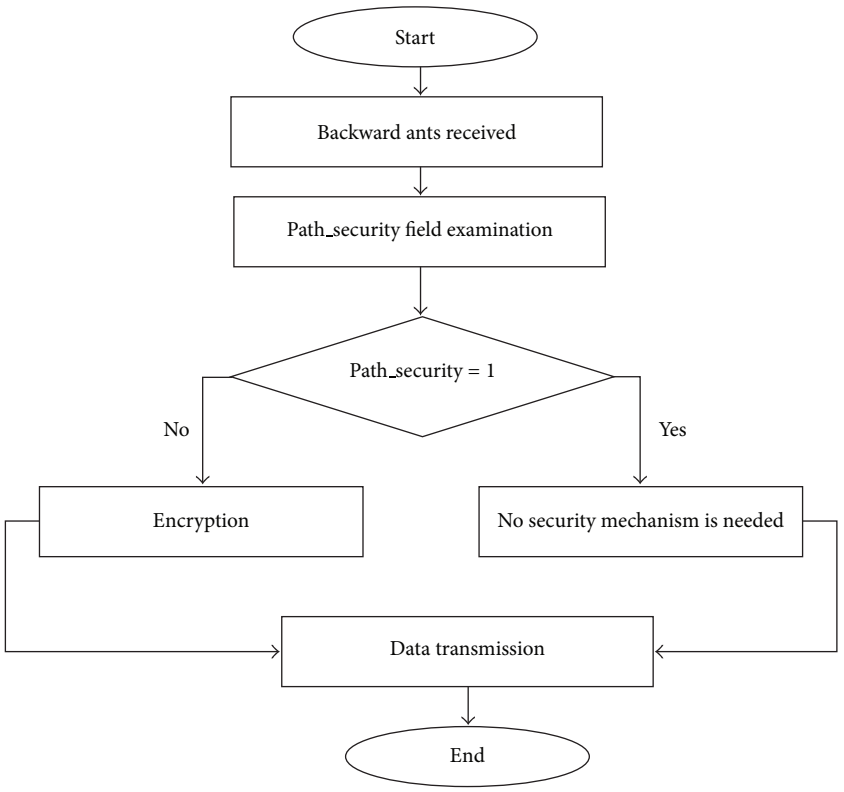

Figure 3: Route selection process.

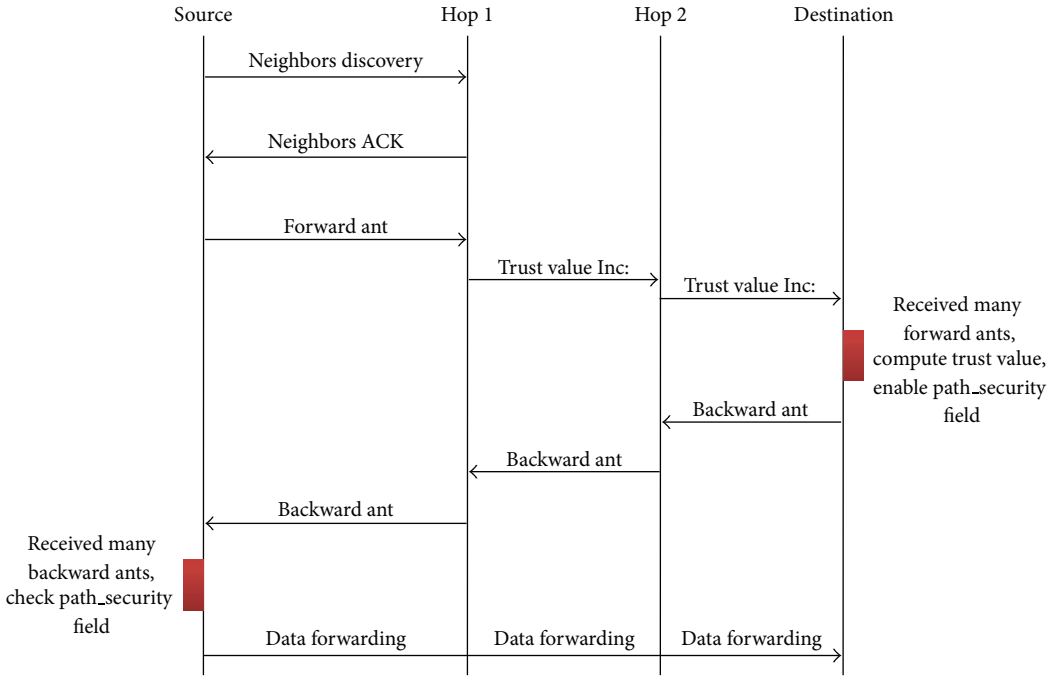

Figure 4: Complete working mechanism of proposed routing protocol.

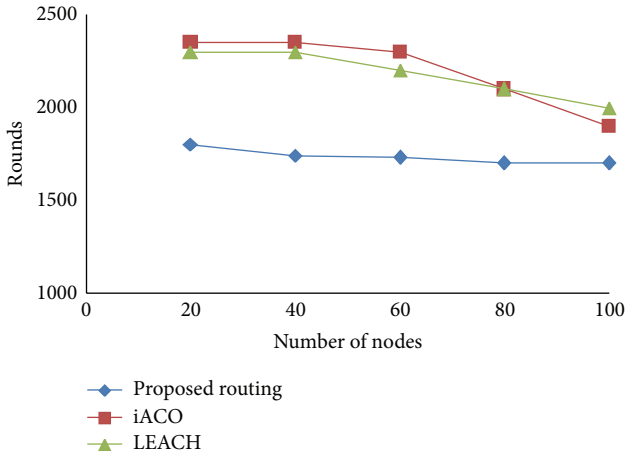

Figure 5: Network life time based on number of rounds.

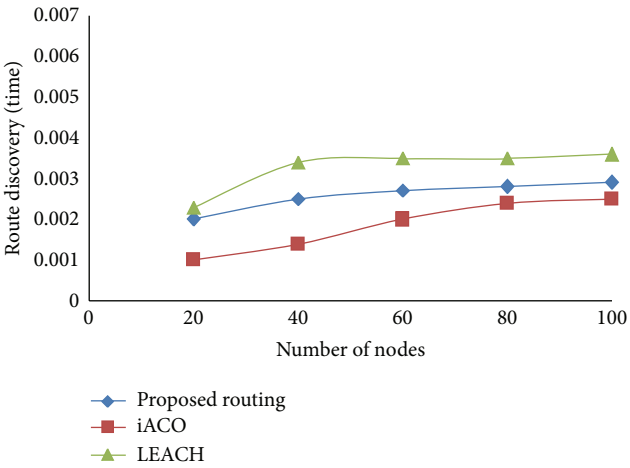

Figure 6: Route discovery efficiency.

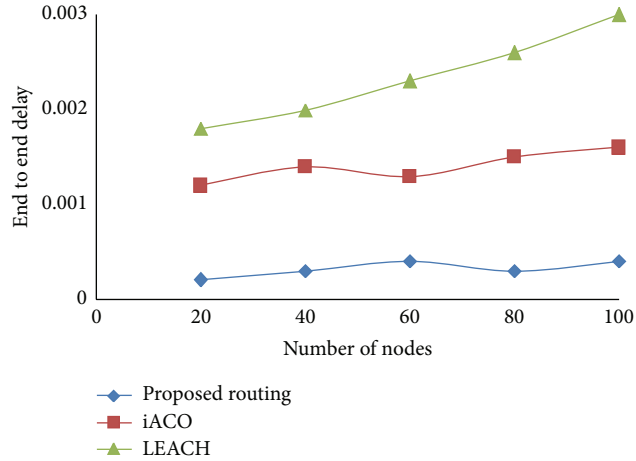

Figure 7: End to end delay.

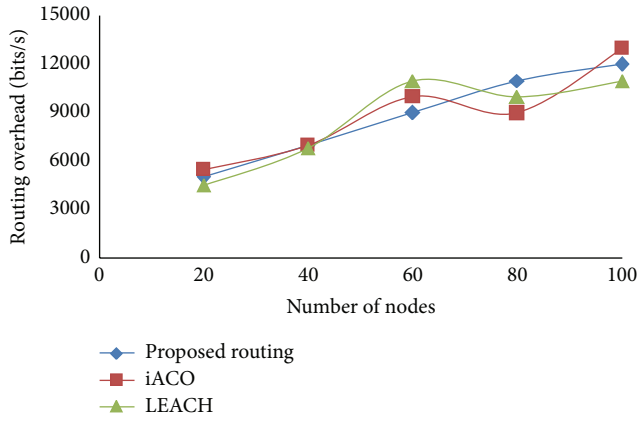

Figure 8: Routing overhead comparison.

4. Performance Evaluation

The performance of ant-based secure routing protocol for WSN is simulated using realistic scenarios. We simulated a WSN having 100 nodes using NS-2. These nodes are randomly deployed in the area of 100 by 100 meters. Initial node energy is set to 6 mJ. Maximum distance between nodes is not more than 20 meters. Each data packet is of 200 bytes. We compared our routing mechanism with low energy adaptive clustering hierarchy (LEACH) and iACO [41]. Figure 5 shows the network lifetime comparison of three routing protocols based on number of rounds.

Initially, the performance of iACO is better than the other; however, as long as the number of nodes increases, iACO shows performance degradation. The proposed routing protocol shows consistent performance in all types of nodes densities. However, overall iACO and LEACH performance is better as compared to our proposal. The reason is that, iACO and LEACH, both are designed to efficiently utilize available energy, while the design goal of our protocol is to ensure security.

In Figure 6, route discovery efficiency in a network of 100 nodes is presented. In this experiment, the performance of iACO is better than the other candidate solutions. The reason is that iACO finds shortest optimal path. LEACH protocol takes more time to find optimal path from source to destination. The reason is that, in LEACH, first data is forwarded to cluster head and then cluster head forwards data to destination after performing data aggregation.

In Figure 7, end to end delay is presented which shows some interesting results. The proposed routing scheme has less end to end delay as compared to LEACH and iACO. The reason is that the proposed routing scheme uses two paths for data transmission, while the other two routing protocols use single path.

Figure 8 compares routing overheads of all three routing protocols with 100 nodes.

All routing protocols have almost similar routing overheads. The proposed routing protocol creates routing overheads due to computation of reputation values, while the rest of two routing protocols create routing overheads by considering energy consumption.

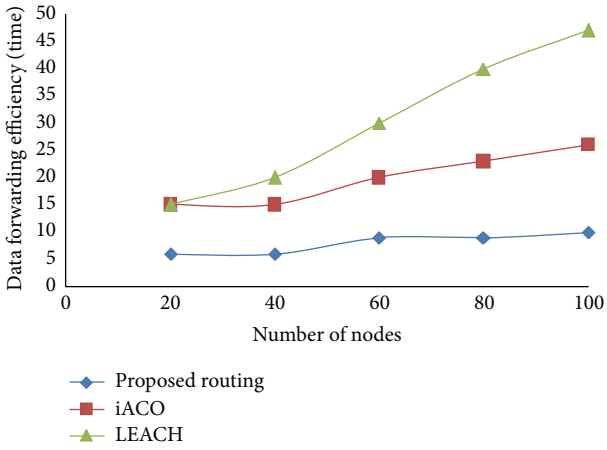

Figure 9: Data forwarding efficiency.

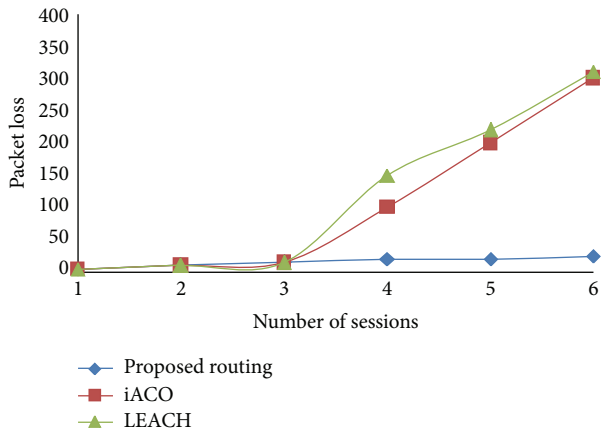

Figure 10: Packet loss in presence of malicious nodes.

In Figure 9, data forwarding efficiency of all protocols is presented. The proposed routing scheme is more efficient and delivers data from source to destination more quickly due to maintenance of two paths.

In Figure 10, few malicious nodes are introduced to observe the packet loss ratio of all the routing protocols. The malicious nodes are used to either drop or misdirect the traffic between source and destination. This simulation is set up in many sessions. Every session is used to forward 400 packets toward destination node. Malicious nodes are introduced from third session onward (i.e., in sessions 4, 5, and 6). In first three sessions, all the routing protocols successfully forward all the packets without any loss. However, when malicious nodes are introduced, most of the packets are either dropped or misdirected by the other routing schemes. However, our proposed mechanism successfully delivered most of the data.

Our routing mechanism is more efficient in presence of malicious nodes due to security mechanism. On the other hand, iACO and LEACH cannot distinguish malicious node in their path, and, that is why packet loss or packet misdirection ratio is very high.

5. Conclusion

Most of WSNs are deployed in harsh and hostile environment, so some sort of security mechanism is highly desirable. Secure routing protocol is an efficient way to ensure security in data forwarding from source to destination. In this paper, we presented in detail a secure routing protocol for WSN which is based on ant colonization technique. We use hello packets for surrounding neighbor's discovery. Our mechanism uses forward ants which collect and increment the reputation values along the path. Similarly, destination node uses backward ants which carry information and instruction from destination node about route security. The proposed mechanism uses two paths for data forwarding not only to overcome the problem of node failure but also to increase the efficiency of overall network.

When compared to other routing protocols such as iACO and LEACH, our proposed routing scheme shows better performance in terms of end to end delay, routing overheads, and data forwarding efficiency. Furthermore, the proposed mechanisms show high data delivery rate in the presence of malicious nodes.

Acknowledgments

The authors extend their appreciation to the Research Centre, College of Applied Medical Sciences, and the Deanship of Scientific Research at King Saud University for funding this research.

References

[1] S. Khan, N. Mast, K. Loo, and A. Silahuddin, "Cloned access point detection and prevention mechanism in IEEE 802.11 wireless mesh networks," *International Journal of Information Assurance and Security*, vol. 3, no. 4, pp. 257–262, 2008.

[2] N. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 374796, 11 pages, 2013.

[3] N. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a Review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[4] S. Khan and K.-K. Loo, "Real-time cross-layer design for large-scale flood detection and attack trace-back mechanism in IEEE 802.11 Wireless Mesh Networks," *Elsevier Network Security*, vol. 2009, no. 5, pp. 9–16, 2009.

[5] S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Computer Networks*, vol. 56, no. 2, pp. 491–503, 2012.

[6] S. Khan, K. Loo, R. Comley, and A. N. Khwildi, "Surveying Ad hoc and Secure Routing in wireless mesh networks," *International Journal of Information Assurance and Security*, vol. 6, no. 1, pp. 73–80, 2011.

[7] S. Khan, K.-K. Loo, N. Mast, and T. Naeem, "SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," *Journal of Network and Systems Management*, vol. 18, no. 2, pp. 190–209, 2010.

[8] S. Khan, K. Loo, and Z. U. Din, "Cross layer design for routing and security in multi-hop wireless networks," *International Journal of Information Assurance and Security*, vol. 4, no. 2, pp. 170–173, 2009.

[9] S. Khan and K. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybridwireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.

[10] N. Meghanathan, "A survey on the communication protocols and security in cognitive radio networks," *International Journal of Communication Networks and Information Security*, vol. 5, no. 1, pp. 19–38, 2013.

[11] M. Radi, B. Dezfouli, K. A. Bakar, and M. Lee, "Multipath routing in wireless sensor networks: survey and research challenges," *Sensors*, vol. 12, no. 1, pp. 650–685, 2012.

[12] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. A. Rashid, "Ant based self-organized routing protocol for wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 42–46, 2009.

[13] M. Frederickson, *A Publication of the National Electronics Manufacturing Center of Excellence*, 2005.

[14] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[15] S. Singh, M. Singh, and D. Singh, "Routing protocols in wireless sensor networks, a survey," *International Journal of Computer Science & Engineering Survey*, vol. 1, pp. 25–34, 2010.

[16] A. M. Popescu, G. I. Tudorache, B. Peng, and A. H. Kemp, "Surveying position based routing protocols for wireless sensor and Ad-hoc networks," *International Journal of Communication Networks and Information Security*, vol. 4, no. 1, pp. 41–67, 2012.

[17] O. Fdili, Y. Fakhri, and D. Aboutajdine, "Impact of queue buffer size awareness on single and multi service real-time routing protocols for WSNs," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 104–111, 2012.

[18] M. Hussaini, H. Bello-Salau, A. Salami, F. Anwar, A. Abdalla, and M. Islam, "Enhanced clustering routing protocol for power-efficient gathering in wireless sensor network," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 18–28, 2012.

[19] A. Kellner, O. Alfandi, and D. Hogrefe, "A survey on measures for secure routing in wireless sensor networks," *International Journal of Sensor Networks and Data Communications*, vol. 1, pp. 1–17, 2012.

[20] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, pp. 55–78, 2009.

[21] K. Xing, "Attacks and countermeasures in sensor networks, a survey," *Springer Network Security*, vol. 7, pp. 534–548, 2005.

[22] V. Kesavan and S. Radhakrishnan, "Multiple secret keys based security for wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 68–76, 2012.

[23] X. Wei, J. Fan, M. Chen, T. Ahmed, and A. K. Pathan, "SMART: a subspace based malicious peers setection algorithm for P2P systems," *International Journal of Communication Networks and Information Security*, vol. 5, no. 1, pp. 1–9, 2013.

[24] M. Azeem, K. Khan, and A. Pramod, "Security architecture framework and secure routing protocols in wireless sensor networks-survey," *International Journal of Computer Science & Engineering Survey*, vol. 2, pp. 189–204, 2011.

[25] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[26] B. Kur, *Secure routing protocols for wireless sensor networks [M.S. thesis]*, University Faculty of Informatics, 2008.

[27] P. Samundiswary, D. Sathian, and P. Dananjayan, "Secured greedy perimeter stateless routing for wireless sensor networks," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, vol. 1, pp. 9–20, 2010.

[28] G. Kumar, I. Titusb, and S. I. Thekkekarab, "A comprehensive overview on application of trust and reputation in wireless sensor network," *Procedia Engineering*, vol. 38, pp. 2903–2912, 2012.

[29] D. Khurana and M. Singla, "Secure and authenticated source routing in wireless networks," *International Journal Of Computer science*, vol. 12, no. 3, 2012.

[30] Z. Che-Aron, W. F. M. Al-Khateeb, and F. Anwar, "ENFAT-AODV: the fault-tolerant routing protocol for high failure rate wireless sensor networks," in *Proceedings of the 2nd International Conference on Future Computer and Communication (ICFCC '10)*, pp. V1467–V1471, May 2010.

[31] S. Khan, K.-K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 Wireless Mesh Networks," *International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435–440, 2010.

[32] S.-B. Lee and Y.-H. Choi, "A secure alternate path routing in sensor networks," *Computer Communications*, vol. 30, no. 1, pp. 153–165, 2006.

[33] V. Thiruppathy Kesavan and S. Radhakrishnan, "Multiple secret keys based security for wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 4, no. 1, pp. 68–76, 2012.

[34] M. S. Lin, J. S. Leu, W. C. Yu, and K. H. Li, "TBRA: termite based routing algorithm in 3D wireless sensor networks," in *Proceedings of the IEEE 75th Vehicular Technology Conference*, pp. 1–5, 2012.

[35] P. G. Hoolimath, M. Kiran, and G. R. Mohana Reddy, "Optimized tERMITE: a bio-inspired routing algorithm for MANET's," in *International Conference on Signal Processing and Communications (SPCOM '12)*, 2012.

[36] J. A. P. Martins, S. L. O. B. Correia, and J. C. Júnior, "Ant-DYMO: a bio-inspired algorithm for MANETS," in *Proceedings of the 17th International Conference on Telecommunications (ICT '10)*, pp. 748–754, April 2010.

[37] G. A. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: an ant-based hybrid routing algorithm for mobile ad hoc networks," in *Proceedings of the Parallel Problem Solving from Nature (PPSN '04)*, vol. 3242 of *Lecture Notes in Computer Science*, pp. 461–470, Springer, 2004.

[38] L. J. G. Villalba, D. R. Cañas, and A. L. S. Orozco, "Bio-inspired routing protocol for mobile ad hoc networks," *IET Communications*, vol. 4, no. 18, pp. 2187–2195, 2010.

[39] A. Cristina, B. Kochem Vendramin, A. Munaretto, M. Regattieri Delgado, and A. Carneiro Viana, "A Greedy Ant Colony Optimization for routing in delay tolerant networks," in *GLOBECOM Workshops Computing and Processing*, pp. 1127–1132, December 2011.

[40] S. S. Iyengar, H.-C. Wu, N. Balakrishnan, and S.Y. Chang, "biologically inspired cooperative routing for wireless mobile sensor networks," *IEEE System Journal*, vol. 1, no. 1, pp. 29–37, 2007.

[41] V. Mahadevan and F. Chiang, "iACO: a bio inspired power efficient routing scheme for sensor networks," *International Journal of Computer Theory and Engineering*, no. 6, pp. 1793–8201, 2010.

[42] L. B. Ribeiro and M. F. De Castro, "BiO4SeL: a bio-inspired routing algorithm for sensor network lifetime optimization," in *Proceedings of the 17th International Conference on Telecommunications (ICT '10)*, pp. 728–734, April 2010.

[43] N. Chauhan, A. Nain, and D. Srivastava, "A bio-inspired energy efficient routing approach to resolve broken link problem in WSN," *International Journal of Computer Applications*, vol. 48, no. 25, pp. 18–24, 2012.

[44] S. S. Iyengar, H. C. Wu, N. Balakrishnan, and S. Y. Change, "Biologically inspired cooperative routing for wireless mobile sensor networks," *IEEE Systems Journal*, no. 1, pp. 29–37, 2007.

[45] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 66–77, October 2004.

[46] K. K. Lavania, S. M. Tiwari, and S. Batra, "Data encryption in the hostile environment for wireless sensor network using virtual energy and trigger time response protocol," *International Journal of Computer Science Issues*, vol. 8, no. 3, pp. 538–542, 2011.