"Vasile Alecsandri" University of Bacău
Faculty of Sciences
Scientific Studies and Research
Series Mathematics and Informatics
Vol. 22 (2012), No. 2, 37 - 46

SECURE BEE ALGORITHMS FOR ROUTING IN MOBILE AD HOC NETWORKS (MANETS): A SURVEY

MARJAN KUCHAKI RAFSANJANI AND HAMIDEH FATEMIDOKHT

Abstract. The Mobile Ad hoc Networks (MANETs) due to infrastructureless, mobility and limited physical security of nodes are vulnerable to a number of security threats. Hence designing a secure routing protocol has become a popular research topic. Bio/Nature-inspired routing algorithms (Swarm Intelligence) such as BeeAdHoc have been presented for developing routing algorithms for MANETs. In this paper, first, we inspect the security vulnerabilities of BeeAdHoc and then study the presented algorithms for improving the BeeAdHoc, which some of them utilized asymmetric cryptography based on digital signatures and others are based on Artificial Immune Systems (AIS). Afterward, BeeAdHoc with its secure frameworks and classical routing protocols AODV and DSR are compared. Our results show that the iBeeAIS is a suitable candidate for secure routing in MANETs.

1. Introduction and preliminaries

In mobile ad hoc networks, all nodes are mobile and are connected via wireless links without using a fixed infrastructure or centralized administration [1]. The different tasks of this network are distributed between the nodes and each node also plays the role of a router for data packets destined for the other nodes. Nodes in MANETs have limited transmission range and two nodes can communicate directly

Keywords and phrases: Mobile Ad Hoc Networks (MANETs), Swarm Intelligence (SI), Cryptography, Artificial Immune Systems (AIS).
(2010)Mathematics Subject Classification: 90B18, 68M12

with each other only if they are within each other's transmission range. Otherwise, the communication between them has to rely on other nodes [2].

Routing for mobile ad hoc networks is a popular research topic. Routing protocols in MANETs can be classified into three categories: reactive, proactive and hybrid approaches. The primary characteristic of proactive approaches is that each node in the network maintains a route to every other node in the network at all times.

Reactive routing techniques, also called on-demand routing, create routes only when desired by the source node. The characteristics of proactive and reactive routing protocols can be integrated in various ways to form hybrid networking protocols [1].

Since the whole routing scheme is being generated and maintained by the own nodes, without any help of a fixed backbone or a base station, routing protocol can be disrupted due to attacks from intruder nodes [3]. Thus securing routing for mobile ad hoc networks is a significant challenge. Bio/Nature-inspired routing algorithms such as BeeAdHoc have been presented to develop routing algorithms for MANETs. A malicious node can disrupt the normal behavior of BeeAdHoc protocol. So, several security solutions have been proposed for MANET routing protocols, based on public key cryptography and AIS [4].

In public key cryptography each node has a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. One specific node knows the private key while the public key is distributed to all nodes taking part in the communication [5]. The artificial immune systems (AISs) are used in intrusion detection, with some success and in many cases have rivaled or bettered the existing statistical and machine learning techniques [6].

In this paper, the comparison of BeeAdHoc with security frameworks and AODV and DSR protocols is presented. Bee algorithm in nature is explained in section 2. In section 3, BeeAdHoc protocol and its security vulnerabilities are investigated. Then, the proposed secure frameworks for BeeAdHoc are introduced in section 4. In section 5, the different types of routing attacks launched by malicious nodes are explained. In section 6, the proposed approaches are compared, and finally the conclusion is in section 7.

2. Bee algorithm in nature

Bee algorithm is inspired by the foraging principles of honey bees in nature. When the colony needs food, the queen bee separates a population of scout bees to search nectar sources. The scout bees search the neighborhood area to find good sources of food. Their move is totally random and they collect information about a food path. After completing their search, they return to the hive and report their findings by performing a dance called waggle dance. This waggle dance represents the percentage density of food over area and the orientation of search area. The next step in searching food is sending follower bees to the best possible location of food sources to transport the food. So, the foraging principles of honey bees in nature are [7]:

- Generate a population of scout bees.
- Repeat till no results are found: send them to search neighborhood.
- Evaluate the results.
- Select the best possible sites from scout bee areas.
- Select the scout bees with the best quality.
- Re-assign the left-over bees for more scout searches.

3. BeeAdHoc protocol and its vulnerabilities

BeeAdHoc is an energy-efficient routing algorithm for routing in MANETs, inspired by bee behavior. BeeAdHoc is a reactive source routing algorithm and uses two types of agents: scouts to discover new routes and foragers to transport data from source to destination. When a route to a destination is needed, a forward scout is transmitted to all the neighbors of a node with an expanding time to live timer (TTL). The intermediate nodes that receive the scout, append their addresses to the source route of the scout until it arrives at the destination. When the forward scout reaches at the destination then the destination node creates a backward scout by reversing the source route and sends it back to the source. Once a scout returns to its source node, it advertises the route to other foragers and then foragers, which are recruited by using the metaphor of dance, transport data to the destination node. The foragers collect the routing information of the network that is used to compute the dance number, which represents the quality of the path traversed [8].

3.1. **BeeAdHoc security analysis.**

In [9] it is investigated how malicious nodes could disrupt the normal routing behavior of BeeAdHoc and some of attacks on the scout and forager are indicated.

- **Scout related attacks:** scouts discover new routes from source to destination node. A malicious node can modify the source route in a scout; also it can forge a scout by spoofing the source address or inserting fake scout ID, or both.

- **Forager related attacks:** foragers implement the main work in BeeAdHoc algorithm. They carry data packets in their payload and transmitted as unicast packets. A malicious node can modify the forager's source route or launch a forged forager. Also it can modify the routing information, carried by foragers, to spuriously increase the quality of a path.

Consequently tampered or forged bee agents, scout and forager, with fake routes, can disrupt the normal routing behavior and reduce the performance of the network.

4. Security frameworks for BeeAdHoc

In this section, security frameworks for BeeAdHoc which are designed based on cryptography principles and artificial immune systems (AIS) are represented.

4.1. **BeeSec.** Mazhar and Farooq [9] have introduced the BeeSec framework. BeeSec is a secure version of BeeAdHoc that utilized asymmetric cryptography based on digital signatures. In BeeSec, scouts and foragers use digital signatures that are computed based on source address, destination address, packet ID, routing information and so on. Also, integrity of the source route is maintained to ensure preventing malicious node from removing valid node on the route. Consequently, BeeSec prevents tampering and fabrication attacks in BeeAdHoc and it is able to successfully counter the attacks launched against the routing protocol; but however, its extreme large processing and communication overheads make it infelicitous for deployment on battery constrained mobile nodes.

4.2. **BeeAIS.** Mazhar and Farooq [10] have presented BeeAIS that is an Artificial Immune System (AIS) model for securing BeeAdHoc. It is based on self non-self discrimination and uses negative selection for anomaly detection. During its learning phase of 50 seconds, BeeAIS learns the system self and then monitors the system for occurrences of non-self associated with the malicious activity. It uses three types of antigens: (1) scout antigen, (2) two type forager antigens. The scout antigen detects abnormal behavior in the forward and backward scouts and two forager antigens detect anomalies in source route and

routing information carried by a forager. Therefore, BeeAIS can detect previously unknown attacks. But it has mobility limitation, namely when node mobility causes the system self to change, it is unable to learn the changing self; therefore average throughput of BeeAIS is low.

4.3. **BeeAIS-DC.** Mazhar and Farooq [4] have proposed the BeeAIS-DC framework. BeeAIS-DC is the third approach for securing BeeAdHoc that uses danger theory concepts for detecting routing misbehavior. It uses dendritic cells (DCs) to provide the ability to adaptively learn the changing self and overcomes the mobility limitation of BeeAIS. The use of the danger signal prevents the need for an initial learning phase at system start up time. BeeAIS-DC senses the presence/absence of danger in tissues, being able to differentiate between the self and non-self behavior. BeeAIS-DC utilizes scout antigens/detectors that make it able to counter only the scout related attacks on BeeAdHoc.

4.4. **iBeeAIS.** Also Mazhar and Farooq [11] have designed iBeeAIS security framework for BeeAdHoc. IBeeAIS is an integrated AIS security framework for misbehavior detection in BeeAdHoc. Its features enable dynamic learning of the system self and non-self, since in iBeeAIS antigens in a tissue are sampled by DCs and then tissue context is classified as self or non-self. IBeeAIS uses activation of B-cells, which endure affinity maturation for a more focused response against suspected non-self antigens. Due to integrated AIS detection process iBeeAIS can learn the changing non-self through feedback from DCs. Therefore iBeeAIS is able to perform good detection accuracy with low false alarm rates for the scout and forager related attacks.

5. Assumptions and investigated attacks

In [9, 11] five routing attacks by malicious nodes are described.

5.1. **Node topology.** The node topology shown in Figure 1 is used for the introduced frameworks. It is a rectangular area of 1000*500 m^2, where node 0 and 8 are the source and the destination, respectively. There are three distinct paths between Node 0 and Node 8; 0-7-8, 0-5-6-8 and 0-1-2-3-4-8. We observe that the path 0-7-8 is the shortest one and it is discovered first. In contrast, the path 0-1-2-3-4-8 is the longest path.

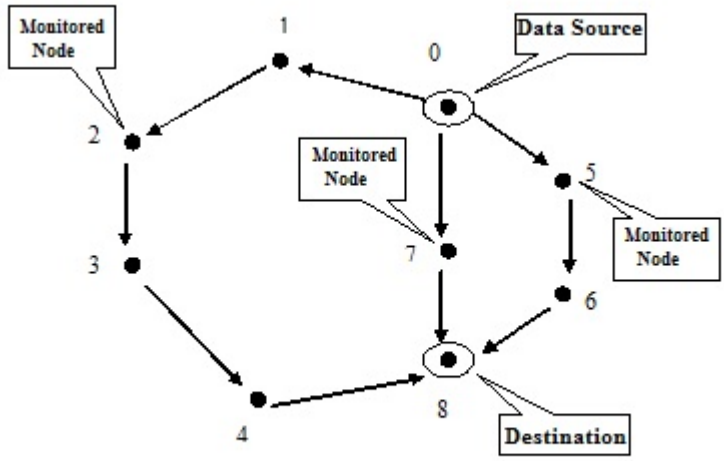

Figure 1. **Node Topology selected for attacks** [9]**.**

5.2. **Routing attacks.** In this section, the details of five attacks launched by malicious nodes are explained [9, 11].

Attack-1: Forging Forward Scout: This attack is launched 100 seconds after the start of simulation, when initial route discovery is complete. The attacker node 4 launches forged forward scouts after 100 s of injection of data into network in order to install a forged route 0-1-2-3-4-8. The fake packets have node 0 as source and node 8 as destination.

Attack-2: Forging Backward Scout: The attack involving spoofed backward scouts is launched by Node 2 at time t = 100 s. Consequently, Node 2 was successfully able to divert subsequent data packets toward itself on the least suboptimal path 0-1-2-3-4-8.

Attack-3: Forging Spoofed Forager: At t = 50 s, the attacker node 5 sends forged foragers to install a forged path 0-1-2-3-4-8 at node 0. The routing information is also modified in forged packets; delay value carried in packet header is artificially reduced to misrepresent the shortest path.

Attack-4: Modifying Forager Route Information: In this attack, the malicious node 7 artificially increases the route delay values in the foragers returning from node 8 to node 0, thus making the path 0-7-8 undesirable. The attack is launched at simulation time t = 100 s.

Attack-5: Returning Scout with a Suboptimal Route: For each received scout, the malicious node 5 changed the source route to 8-4-3-2-1-0 and instead of broadcasting it further, sent it back as a unicast message. As a result, the longer path 0-1-2-3-4-8 got established instead of the desired path 0-5-6-8. This path was set earlier, as a result, more foragers were returned for this path.

As a result of the experiments carried out in [9, 11], BeeSec and iBeeAIS successfully countered the five introduced attacks.

6. Comparing Security frameworks for BeeAdHoc

A summary of the comparison of frameworks presented so far and AODV and DSR, which are reactive routing protocols, is shown in Table 1. The following comparison criteria are used.

- **Energy expenditure:** energy consumed in transporting one kilobyte of data to its destination.
- **Success rate:** the ratio between the number of packets successfully received by the application layer of a destination node and the number of packets originated at the application layer of each node for that destination.
- **Delay:** time interval once a data packet is generated by the application in a node and when it got delivered to the application layer of a destination node.
- **Throughput:** the total number of data bits delivered to destination nodes during the simulation divided by the total simulation time.
- **Transmission efficiency:** the number of data bytes delivered to the application layer at destination nodes at the cost of a unit control byte.
- **Average control overhead:** The total number of control bytes (Mbytes) transmitted by all nodes in the network.

7. Conclusions

In this paper, we studied BeeAdHoc protocol, which is inspired by bee behavior, and its vulnerabilities against routing attacks. Then the security frameworks for BeeAdHoc are reviewed: some of them use asymmetric cryptography based on digital signatures and the others use artificial immune systems (AIS) for counter to attacks. The frameworks introduced and AODV and DSR, which are reactive routing protocols, were compared. According to Table 1, BeeAdHoc has the same/better performance as AODV and DSR. This analysis shows

that iBeeAIS enhances the classical AIS algorithm and is able to perform anomaly detection in MANETs that have no fixed definitions of self or non-self. Also security of iBeeAIS protocol is the same as compared to BeeSec, but with very small processing and communication overheads.

Acknowledgment. The authors would like to express their thanks to anonymous referees for their comments and suggestions which improved the paper.The authors have been supported by Mahani Mathematical Research Center of Shahid Bahonar University of Kerman, Iran.

References

[1] S. Basagni, M. Conti, S. Glordano and I. Stojmenovic, **Mobile Ad Hoc Networking**, *IEEE Press book*, 2004.
[2] M. Ilyas, **Ad Hoc Wireless Networks**, CRC Press book, 2003.
[3] L.Venkatraman and D.P.Agrawal, **Strategies for enhancing routing security in protocols for mobile ad hoc networks**, J.Parallel and Distributed Computing, 63(2003), 214-227.
[4] N. Mazhar and M. Farooq, **A sense of danger: Dendritic cells inspired artificial immune system (AIS) for MANET security**, Proceedings of the ACM Genetic and Evolutionary Computation Conference, 2008.
[5] A. MS, **Public Key Cryptography - Applications Algorithms and Mathematical Explanations**, Tata Elxsi Ltd, 2007.
[6] U. Aickelin, J. Greensmith and J. Twycross, **Immune system approaches to intrusion detection-a review**, Artificial Immune Systems, 2004.
[7] S. K. Dhurandher, S. Misra, P. Pruthi, S. Singhal and S. Aggarwal, **Using bee algorithm for peer-to-peer file searching in mobile ad hoc networks**, J.Network and Computer Applications, 34(2011), 1498-1508.
[8] H. F. Wedde, M. Farooq, T. Pannenbaecker, B. Vogel, C. Mueller, J. Meth and R. Jeruschkat, **BeeAdHoc: An energy efficient routing algorithm for mobile ad hoc networks inspired by bee behavior**, Proceedings of the ACM Genetic and Evolutionary Computation Conference, (2005), 153-160.
[9] N. Mazhar and M. Farooq, **Vulnerability analysis and security framework (BeeSec) for nature inspired MANET routing protocols**, Proceedings of the ACM Genetic and Evolutionary Computation Conference, (2007), 102-109.
[10] N. Mazhar and M. Farooq, **BeeAIS: Artificial immune system security for nature inspired, MANET routing protocol, beeadhoc**, Proceedings of the International Conferences on Artificial Immune Systems, (2007), 370-381.
[11] N. Mazhar and M. Farooq, **A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols**, J.Applied Soft Computing, 11(2011), 5695-5714.

TABLE 1. Comparison of discussed frameworks, AODV and DSR routing protocols

	BeeAdHoc	BeeSec	BeeAIS	BeeAIS-DC	iBeeAIS	AODV	DSR
Used method	Inspired by bee behavior	Digital signature	Negative selection based AIS	Dendritic cells inspired AIS and using the danger theory	Using light-weight AIS model with pre-activated B-cells	—	—
Energy expenditure	Low	Low	Low	Low	Low	High	Very high
Success rate	High	High	High	High	High	Low	Higher than others
Delay	Low	Low	Low	Low	Low	High	Very high
Throughput	High	High, but lower than BeeAd-Hoc	Low	Lower than BeeAd-Hoc, higher than BeeSec	Higher than BeeAd-Hoc	Lower than others except BeeAIS	Low
Transmission efficiency	Low	Very low	low	Low	Low	Low except BeeSec	Very low
Average control overhead	Low	Very low	Low	Low	Low	Higher than others except BeeSec	Higher than BeeSec
Ability of doing well in case of non-changing self	—	—	Is able to prevent attacks	Is able to counter the scout related attacks	Is able to detect previously unseen attacks by better performance than others	—	—
Ability to adaptively learn the changing non-self	—	—	Is unable to detect such attacks	Is unable to detect such attacks	Is able to detect and prevent such attacks	—	—
Ability to adaptively learn the changing self	—	—	Is unable to learn the changing self	Is able to learn the changing self	Is able to learn the changing self	—	—

Marjan Kuchaki Rafsanjani
Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran, e-mail: kuchaki@uk.ac.ir.

Hamideh Fatemidokht
Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran, e-mail: fatemi1367@yahoo.com.