ACCEPTED FROM OPEN CALL

N-HOP NETWORKS: A GENERAL FRAMEWORK FOR WIRELESS SYSTEMS

TONGTONG LI, MAI ABDELHAKIM, AND JIAN REN

ABSTRACT

This article introduces a unified framework for quantitative characterization of various wireless networks. We first revisit the evolution of centralized, ad-hoc and hybrid networks, and discuss the trade-off between structure-ensured reliability and efficiency, and ad-hoc enabled flexibility. Motivated by the observation that the number of hops for a basic node in the network to reach the base station or the sink has a direct impact on the network capacity, delay, efficiency and their evaluation techniques, we introduce the concept of the N-hop networks. It can serve as a general framework that includes most existing network models as special cases, and can also make the analytical characterization of the network performance more tractable. Moreover, for network security, it is observed that hierarchical structure enables easier tracking of user accountability and malicious node detection; on the other hand, the multi-layer diversity increases the network reliability under unexpected network failure or malicious attacks, and at the same time, provides a flexible platform for privacy protection.

PREFACE

Communications rely on networks. Today's wireless networks are generally divided into two categories: centralized networks with well-defined infrastructure, and distributed or ad-hoc networks which are virtually structureless. There is also a trend to blend these two structures together, resulting in various hybrid networks. In this article, we summarize the general design criteria of wireless networks, and present a unified framework that can capture existing systems as special cases. This unified framework also makes quantitative characterization of wireless networks more tractable. To this end, we first examine some representative systems in the literature.

EVOLUTION OF WIRELESS COMMUNICATION SYSTEMS

The development of mobile telephony traces back to the late 1910s, when a group of German engineers started the experiments on telephony via radio links, and tested on the military trains between Berlin-Zossen in 1918. The first handheld radio transceivers, also called walkie-talkies, were the backpacked Motorola SCR-300, developed in 1940 and later refined and widely used during the World War II. Shortly thereafter, engineers in Bell Labs developed a system to allow mobile users to place and receive telephone calls from automobiles, leading to the inauguration of mobile services in 1946 in St. Louis, Missouri. From thereon, a wide range of incompatible mobile services, supported by analog techniques, were provided in urban areas, each offering very limited coverage through a base station that has only a few channels.

CELLULAR SYSTEMS

The concept of cellular technology, which exploited low-power transmitters and allowed wide area service through frequency reuse, was introduced and developed by Bell Labs engineers from the late 1940s to early 1970s [1]. While the first hexagonal cell concept was proposed in 1947, the full development and implementation of the cellular technology, including both frequency reuse and call handover, took more than two decades. The cellular technology made the mobile services affordable to ordinary people, and led to the revolutionary spread of wireless communications.

The first generation (1G) cellular systems (1970s), represented by AMPS (Advanced Mobile Phone System) in the US (later on evolved to IS-41) and ETACS (European Total Access Communication System) in Europe, relied on analog technologies and mainly provided voice services. Started in late 1980s and deployed in 1990s, the second generation (2G) cellular systems (United States Digital Cellular (USDC) IS-136, CDMA IS-95, and GSM) all used digital coding and modulation techniques. The 2G systems increased the network capacity by about three times. As they were designed before the wide spread of the internet, they mainly supported voice-centric services and limited data-services, like short messages, paging and Fax.

Began in late 1990s, the 3G systems (UMTS WCDMA, CDMA 2000, and TD-SCDMA) supported high-speed multimedia services and seamless global roaming. Wireless access became available throughout the earth, with the proud claim of "anywhere, anytime, anything". The communication quality was further enhanced by the OFDM technique, leading to the high speed,

Tongtong Li, Mai Abdelhakim, and Jian Ren are with Michigan State University.

 1536-1284/14/$25.00 © 2014 IEEE

high quality 4G systems, represented by WiMAX (Worldwide Interoperability for Microwave Access) and LTE (Long Term Evolution). Today, with the coexistence of 3G and 4G, we can have real-time multimedia communications through world-wide networks.

Ad-Hoc Networks

The walkie-talkies, which are still widely used today in military, public safety, businesses, outdoor recreation and the like, actually form a complete mesh network, where any two users within the device power range can communicate directly in a structureless manner.

Going beyond this one-hop communication mode and allowing multihop routing process, the self-configuring infrastructureless wireless ad-hoc network has attracted lots of attention from the research community. The research on ad-hoc networks was mainly driven by the growth of laptops and 802.11/Wi-Fi wireless networking, and the advent of all kinds of wireless sensors, leading to the areas of MANET (Mobile Ad-hoc Network) and WSN (Wireless Sensor Network), respectively. MANET has been widely deployed as local area networks in businesses, universities, airports and places alike, for convenient wireless internet access and internet-assisted communications. At the same time, wireless sensor networks have seen wide use in both military and civilian applications, such as health monitoring, intelligent transportation systems, target detection and tracking, especially in unattended and possibly hostile areas.

The Merging Ground for Cellular and Ad-Hoc — Hybrid Networks

While the structureless ad-hoc networks provide excellent flexibility with reliable performance for small scale networks, scalability proved to be a serious challenge for large-scale ad-hoc networks due to the uncertainty, complexity, as well as the delay and energy concerns in the routing process. The problems become even worse when the devices are mobile.

This observation leads to ad-hoc networks with local structures, known as *hybrid networks*. One representative example is the clustered wireless sensor networks, where the sensors are grouped into clusters, with each cluster managed by a cluster head in a centralized manner. The routing responsibility is fulfilled only by the cluster heads, but not the ordinary sensor nodes. Similar ideas are developed for the mobile ad-hoc network (MANET) [2], include multi-hop cellular network (MCN), integrated cellular and ad-hoc relaying systems (iCAR) [3], self organizing product radio networks (SOPRANO) [4], etc.

At the same time, hybrid networks also raised from the cellular networks. This is mainly motivated by the following two observations:

- For today's centralized network, the mobile will generally lose network connection once the BS is not functioning, since each mobile is typically connected to only one BS.
- Even if two mobiles are spatially close, they cannot establish direct communication, but have to communicate through the BS, leading to unnecessary resource waste. That is, traditional centralized network does not have sufficient diversity and endpoint communication flexibility.

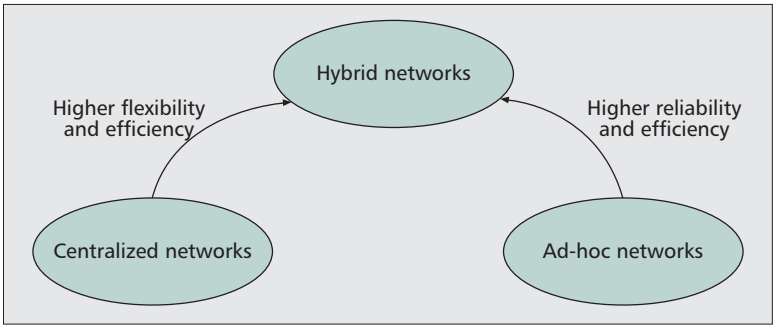

Figure 1. Merging of centralized and ad-hoc networks.

As a result, recent wireless MAN and LAN standards, such as WiMAX 802.16 and WiFi 802.11s, have incorporated the mesh capability to the wireless network nodes, which allows each node to forward the traffic of other nodes in the network in a planned yet ad-hoc manner.

Other representative examples include Ad-hoc GSM (A-GSM) [5], cellular networks with device-to-device (D2D) communications [6], and iCAR [3], where the main idea is to improve transmission flexibility, viability, capacity, and traffic balance by allowing device-to-device and/or device-to-relay station communications.

From the discussions above, it can be seen that hybrid networks serve as a merging ground for centralized and ad-hoc networks, as shown in Fig. 1. Hybrid networks stimulate the research on different kinds of heterogeneous networks.

General Design Criteria

The evolution of the centralized and ad-hoc networks to hybrid networks reveals that: for wireless communications, we would need both network centric management as well as ad-hoc flexibility. Based on this observation, we can summarize the general network design criterions as follows:

The network needs to have a well-organized infrastructure to ensure the reliability (including both transmission accuracy and security), capacity, energy efficiency as well as time efficiency. At the same time, the network should provide sufficient flexibility by allowing authorized ad-hoc communications among the nodes or devices. More specifically,

- The infrastructure needs to be hierarchical for efficient management. The density of the devices gets higher as their level gets lower.
- The infrastructure needs to provide sufficient diversity at each level to combat hostile attacks or unexpected system failures. More specifically, devices or basic nodes (BNs) at each level can communicate with two or more upper level devices.
- The infrastructure needs to provide sufficient flexibility.
  - –Once authenticated, neighboring devices (either relay stations or basic nodes) at the same level can communicate directly with each other within their transmission range without going through higher layer nodes.

The circulatory system in the human body is an excellent combination of a well-structured "backbone" network and numerous small ad-hoc networks at the endpoints. It ensures transmission efficiency, diversity and endpoint service flexibility, and thus provides a very good example for network design.

–When permitted, each device can communicate directly with higher layer nodes within its communication range to minimize the number of hops needed to reach a base station (BS) or sink.
–Under special cases when a BN cannot access the network directly, as long as an agreement is reached between two BNs (both BN should be authenticated if possible), one BN can serve as the relay for another BN.

From a biomimetic perspective, these criterions can be largely verified in the design of the human body. Consider the circulatory system, in which the extracellular fluid is transported through parts of the body in two stages [7]. The first stage is the movement of the blood in the blood vessels; the second stage is the movement of fluid between the blood capillaries and the intercellular space between the tissue cells. The latter stage is also called micro-circulation, it is for the transport of nutrition to the tissues and removal of cell excreta. The first stage is centralized and well structured with good diversity. Even if some vessels are not functioning well (e.g. blocked), as long as they are within a certain threshold, the human body will continue to function. In the second stage, the micro-circulation, the exchange of water, nutrients and other substance between the plasma in blood and interstitial fluid in the tissue is mainly done through diffusion, which results from thermal motion of the water molecule and dissolved substances in the fluid. To make it short, it is random!

As can be seen, the circulatory system in the human body is an excellent combination of a well-structured "backbone" network and numerous small ad-hoc networks at the endpoints. It ensures transmission efficiency, diversity and endpoint service flexibility, and thus provides a very good example for network design.

The Concept of N-hop Networks

With the general design criterions in mind, we now try to come up with a unified framework for wireless networks that could cover most of the existing systems as special cases, and makes quantitative network characterizations (such as throughput, delay, and efficiency) more tractable.

We first look at some examples. In strictly centralized networks, which is widely adopted in cellular communication systems, the mobile reaches the base station (BS) in one hop. In the one-layer relay-assisted cellular networks, the mobile either reaches the BS directly in one hop, or reaches the base station through a relay in two hops. In pure ad-hoc networks or sensor networks, there is generally no specific limit on the number of hops for a basic node to reach a sink.

For any wireless network, let the minimum number of hops for a basic node (i.e., the terminal, such as a mobile or a sensor) i to reach the base station (BS) or the sink be N_i. Define $N = \max N_i$ over all the nodes. N is an important characterization on how closely the basic nodes are connected to the BS or the sink. It has a direct impact on network capacity, reliability, delay, efficiency, as well as their evaluation techniques.

Now we are ready to introduce the concept of N-hop networks. A wireless network is said to be an N-hop network if every basic node (BN) can reach the BS or the sink within N hops under normal network conditions. By normal conditions, we mean that there are no hostile attacks, or severe, unexpected system failures. Based on this definition, if $N = 1$, we obtain the strictly centralized network. For some sensor networks with mobile access points, we also have $N = 1$, see the SENMA in [8] for example. In SENMA, with well designed mobile access trajectory, there is no routing and all the sensors can reach the mobile access in one hop. If $N = 2$, we get the relay-assisted cellular network; For an ad-hoc network of size N, generally, $N \le n - 1$. Actually, almost all the existing systems fall into this unified framework. As will be seen later, with this framework, analytical evaluation of the throughput, delay, and efficiency becomes more tractable.

Denote the total number of hops for a node i to reach its destination, node j, as $N_{i,j}$. For an N-hop network, we have $1 \le N_{i,j} \le 2N + N^c_{i,j}$, where $N^c_{i,j}$ is the number of hops required for the inter-cell communications between the two base stations connected to nodes i and j, respectively. For the complete (local) mesh network where any two nodes can communicate directly, we always have $N_{i,j} = 1$ for any source-destination pair (i, j).

Due to possible link failure conditions and/or malicious attacks, the number of hops for a node to reach the sink could be more than N. For this reason, we extend the definition of N-hop networks to α-*level N-hop networks*, which is characterized by: $Pr\{\text{BN can reach the BS or sink within } N \text{ hops}\} = \alpha$. The level α can be used as an indicator of how smooth the network is operating.

Next, we provide two examples to further illustrate the N – hop network: one on mobile network, and one on sensor network.

Example 1: A 3-Hop Mobile Network

In this network, multiple base stations (BSs) and two levels of relay stations (RSs) (level 1 and level 2) are employed to serve the basic nodes (BNs) - the mobiles, as illustrated in Fig. 2. Level 1 RSs have larger coverage area and storage capacity than level 2 RSs, but level 2 RSs have much higher distribution density in the network. Devices or nodes at each level can communicate with two or more upper level devices. Within their transmission range, neighboring devices (either RSs or BNs) at the same level can communicate directly with each other without going through higher layer nodes. At the same time, each device can communicate directly with the highest level higher layer nodes within its communication range to minimize the number of hops needed to reach a BS. This is a 3-hop network. The tolerance of the network to system failures or hostile attacks is determined by its inherent diversity.

Example 1 is easy to understand because it relies on the deployment of the base stations and the relay stations. A more interesting case would be the hop number control in sensor networks. The next example provides a mobile

access coordinated N-hop wireless sensor network (MC-WSN) architecture for reliable and efficient information exchange. This design is motivated by Sensor Networks with Mobile Access Points (SENMA) [8]. In conventional sensor networks with mobile access points (SENMA), the mobile access points (MAs) traverse the network to collect information directly from individual sensors. While simplifying the routing process, a major limitation with SENMA is that a transmission is made only if an MA visits the corresponding source node; thus, data transmission is limited by the physical speed of the MAs and the length of their trajectory, resulting in low throughput and huge delay. In an effort to solve this problem and find an efficient solution for time-sensitive information exchange, we proposed the MC-WSN architecture based on the recent advances in Unmanned Aerial Vehicles (UAVs), which have been used for network deployment and coordination functions in sensor networks [9].

Example 2: Mobile Access Coordinated Wireless Sensor Network (MC-WSN)

In MC-WSN, the whole network is divided into cells, each is covered by one MA and is served with powerful center cluster head (CCH) located at the middle of the cell, and multiple ring cluster heads (RCHs) that are distributed to minimize the average number of hops for the BN to reach the MA. The MAs coordinate the network through deploying, replacing and recharging the nodes. They are also responsible for enhancing the network security, by detecting compromised nodes then replacing them.

Data transmission from sensor nodes to the MA goes through simple routing with the CCH or the RCHs. Through active network deployment and topology design, the number of hops from any sensor to the MA can be limited to a *pre-specified number N* [9]. The MC-WSN architecture is shown in Fig. 3.

The main advantages of MC-WSN lie in the multi-functionality of the mobile access, the hop number control through topology design, and the hierarchical and heterogeneous sensor deployment. MC-WSN has the following features:

- Resolving the network deployment problem and being able to actively prolong the network lifetime.
- Being applicable for time-sensitive applications.

Unlike in SENMA, the delay in MC-WSN is independent of the physical speed of the MA, and is effectively managed through hop number control.

- Enhancing network security.

The MAs can detect malicious SNs and CHs and replace them [10].

- Providing high energy efficiency.

In the proposed MC-WSN, SNs only communicate with their nearest CHs, and are not involved in any inter-cluster routing. Overall, the MC-WSN enhances the network resilience, reliability and scalability.

The examples above illustrate that the *N*-hop network does provide a general framework for the characterization of centralized, ad-hoc, as well as hybrid networks.

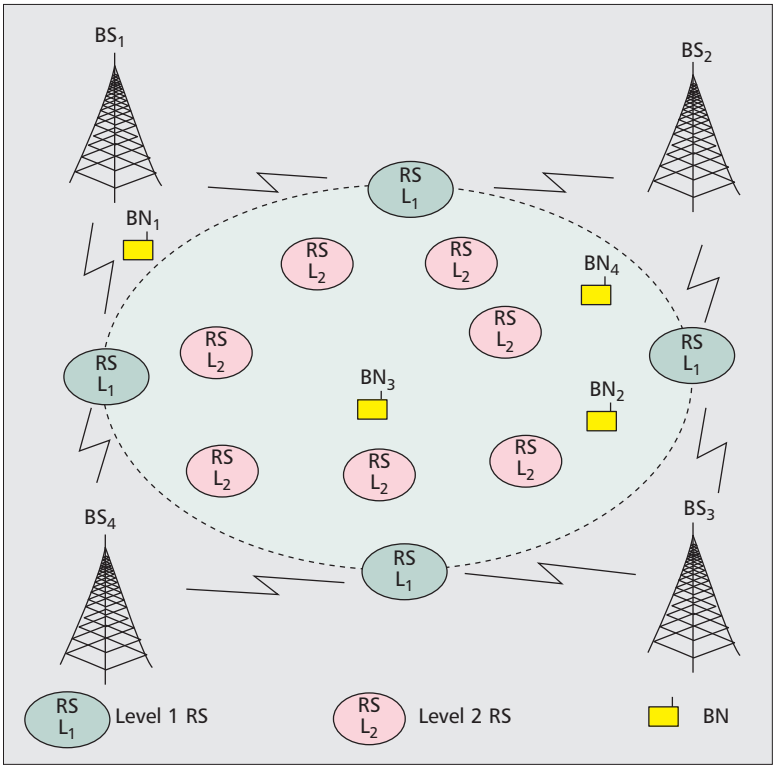

Figure 2. Example 1. A 3-hop mobile network.

Analytical Evaluation of the Network Performance

In this section, we provide a quantitative characterization of wireless networks under the N-hop framework, in terms of throughput, delay, and energy efficiency.

Throughput

Consider an N-hop network that contains N basic nodes. For each individual BN i, the throughput, $T(i)$, is defined as the average number of packets per slot that are initiated by node i and successfully delivered to the intended receiver [11]. For an N-hop network, when the receiver is the BS or the sink, the number of hops from BN i to the BS satisfies $1 \le N_i \le N$. Note that the transmission can always go through different paths due to the existence of network diversity. We assume that for each hop number $l \in \{1, 2, \ldots, N\}$, there are $P_{i,l}$ possible l-hop paths from BN i to the BS. Let $T(i|N_i = l, \mathcal{P}_i = p)$ be the throughput that can be achieved along one of the l-hop paths $\mathcal{P}_i = p$, then the throughput of node i can be calculated as:

$$T(i) = \sum_{l=1}^{N} \sum_{p=1}^{\mathcal{P}_{i,l}} T\left(i \middle| N_i = l, \mathcal{P}_i = p\right) \Pr\{\mathcal{P}_i = p \middle| N_i = l\} \times \Pr\{N_i = l\}. \quad (1)$$

The overall network throughput can be obtained as $\Sigma_{i=1}^{n} T(i)$.

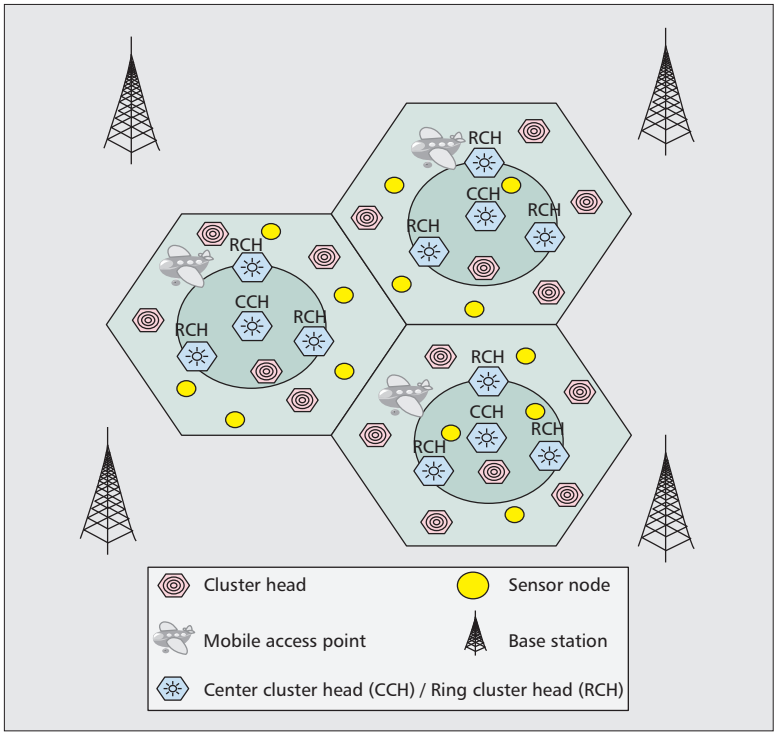

Figure 3. Example 2. A mobile access coordinated wireless sensor network.

It should be noted that the throughput of node i along path $\mathcal{P}_i = p$, $T(i|N_i = l, \mathcal{P}_i = p)$, mainly depends on the probability of successful transmission at each hop, which is generally characterized by the probability that the signal to noise and interference ratio (SINR) is above a certain threshold γ [12]. Assume a relatively flat noise power along the transmission path, when the transmission power of the nodes is low, the throughput improves as the number of hops increases. This is due to the reduced path loss at each hop as compared to longer distance transmission. On the other hand, when the transmission power is large, the throughput improves as the number of hops decreases, because of reduced propagation errors. This is illustrated in Fig. 4, where the per-node throughput versus the transmit signal to noise power ratio is shown.

From the discussions above, we can see that under a particular power constraint, there exists an optimal number of hops for throughput maximization, as illustrated in Fig. 4. This result indicates that: the optimal hop number versus the transmission power can serve as a critical reference for network structure design.

Delay

The quantification of the delay in N-hop networks involves both information theory and queuing theory. The former studies the maximum rate at which each node can transmit over the channel, by considering noise and interference effects, but ignoring the queuing delay that could be experienced at intermediate relays/queues. The latter considers the queuing delay with possible random arrival and departure times at the intermediate relays.

The delay in one-hop communication is mainly composed of three parts:

- The *queuing delay* is the time between the packet arrives at a node, until it reaches the head of the queue where it can be transmitted. Little's theorem [13] formulates the average queuing delay as

$$D_q = \frac{Q_L}{\lambda_q},$$

where Q_L is the average number of packets in the queue, and λ_q is the rate at which the packets arrive to the queue.

Nodes with finite storage can be modeled as M/M/1/B queues [13], where the arrivals are memoryless Poisson process with rate λ_q, the departure times are exponentially distributed with departure rate ϑ, and the storage of each queue is B packets. Let $\mathbb{P}_B$ be the probability that the queue is full. Note that each node receives a packet only when it is not full, hence the effective arrival rate is $\lambda_e = \lambda_q (1 - \mathbb{P}_B)$. With the effective arrival rate and the mean queue length, the queuing delay can then be obtained using the Little's theorem.

- The *back-off delay* occurs when a packet is not successfully received due to either full receiver buffer or collisions in the transmission; in this case, the transmitter will retransmit the packet after a back-off time. In structured networks, back-off time can be minimized due to the presence of a centralized control on data transmission, which allows interfering nodes to transmit on a different time slots or different frequency bands.
- The *transmission delay* is the difference between the time data is encoded and transmitted until it is successfully recovered/decoded at the receiver. It depends on the size of the packet and the transmission rate, and is bounded by the information-theoretic capacity.

In an N-hop wireless network, the average delay of a transmission, $\overline{D}$, can be calculated as:

$$\overline{D} = \sum_{l=1}^{N} \sum_{p=1}^{\mathcal{P}_{i,l}} \sum_{m=1}^{l} \overline{D}_{p,m} \Pr\{\mathcal{P}_i = p | N_i = l\} \Pr\{N_i = l\}, \quad (2)$$

where N_i denotes the actual number of hops for a transmission, and $\overline{D}_{p,m}$ is the average delay in the mth hop along path p.

Example 3: Delay in Sensor Networks

In this example we compare the average end-to-end delay for two network models:

- The SENMA architecture, which is a one-hop centralized network with mobile access
- The MC-WSN architecture (Example 2) with $K = 3$ RCHs and shortest path routing.

Assuming that the nodes are uniformly distributed, and the cell radius is d_{cell}.

In MC-WSN, the ring radius along which the RCHs are placed is $R_t = 0.233\, K \sin(\pi/K)\, d_{cell}$, which is obtained to minimize the average number of hops from any CH to a sink. The average number of hops can be obtained by dividing the average distance to the sink over the average per-hop distance. In SENMA, we assume that the speed of the MA can be as high as $v = 30$m/s.

The effect of the cell radius d_{cell} on the average delay for the two network models is illustrat-

ed in Fig. 5. As can be seen, the structured MC-WSN achieves several orders of magnitude lower delay when compared to SENMA, as the delay in SENMA is mainly determined by the physical speed of the MA.

Energy Efficiency

To evaluate the energy efficiency, we use the circuitry radio energy dissipation model [14]. In this model, each receiving node consumes E_{rx} (J/bit), and each transmitting node consumes $E_{tx} + \varepsilon_{pa} L^{\beta}$ (J/bit), where ε_{pa} is the energy consumed by the power amplifier, β is the path loss exponent, L is the per-hop distance, and E_{tx} is the energy dissipated in the transmitter electronics. Then the total energy dissipated at a one-hop communication is $E_{tx} + \varepsilon_{pa} L^{\beta} + E_{rx}$ (J/bit).

In an N-hop network, the average energy consumption for a packet transmission, $\overline{E}$, can be calculated as:

$$\overline{E} = \sum_{l=1}^{N} \sum_{p=1}^{\mathcal{P}_{i,l}} \sum_{m=1}^{l} \overline{E}_{p,m} \Pr\{\mathcal{P}_i = p \,|\, N_i = l\} \Pr\{N_i = l\}, \quad (3)$$

where $\overline{E}_{p,m}$ is the average energy consumed at the mth hop of path p.

Example 4: Energy Efficiency vs. the Number of Hops

In this example, we compare the average energy dissipation of SENMA and MC-WSN, under the same setting as in Example 3. The result is shown in Fig. 6. It is clear that the N-hop MC-WSN is much more efficient than SENMA networks. The reason is that in SENMA, each SN must first receive a beacon signal from the MA in order to report its data. All sensors within the coverage area of the MA receive the beacon signal, and only one sensor responds each time [8]. The energy dissipation during the beacon reception process contributes significantly to the overall energy consumption for each transmission in SENMA.

Remark

For the α-level N-hop network, the number of hops can be greater than N with probability $(1 - \alpha)$. In this case, we can extend Eqs. 1–3 accordingly, by changing N to N_{max}, which is the maximum number of hops in a cell. Equations 1–3 can also be extended directly to the node-to-node communication case.

Security Perspectives

Delay-Assisted Network Failure/Attack Detection

Consider a particular node i, under normal network conditions, N_i is the number of hops from BN i to the sink, then the delay of node i's transmission to the sink is $D_i = \Sigma_{k=1}^{N_i} d_k$, where d_k is the delay in hop k. Note that the average delay is given in Eq. 2. If the actual delay D_i is much larger than the average delay $\overline{D}_i$, then this indicates that either additional hops are utilized at the data delivery, or there is an unexpected large back-off time. In other words, the ratio between the actual delay and the average delay of a transmission can be used as an indicator for the detection of unexpected network failures or hostile attacks.

When network synchronization is achieved, the detection of network failure problems can be implemented by including a time stamp in each packet representing the transmission time of the

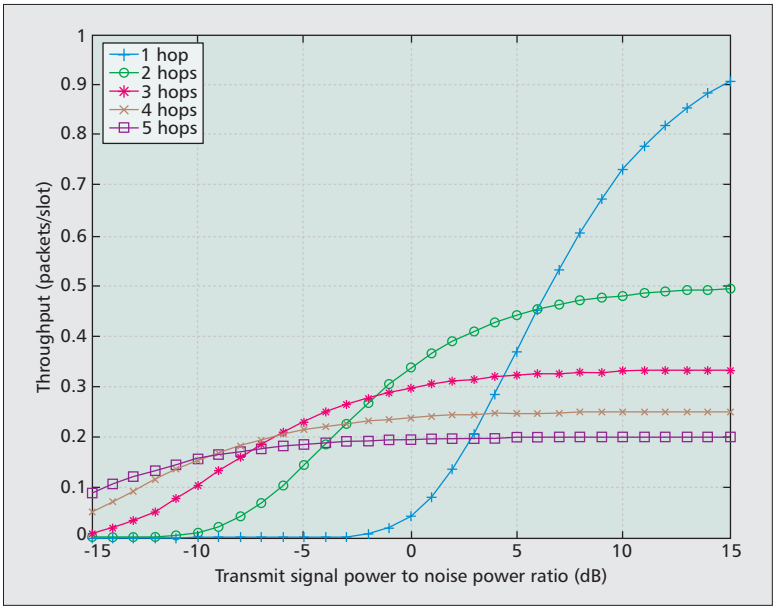

Figure 4. Per-node throughput $T(i|N_i, \mathcal{P}_i)$ vs. the average transmit power to noise power ratio for different number of hops, assuming AWGN channel, path loss exponent is 4, SINR threshold is $\gamma = 5$dB, the hops are equidistant, distance between transmitter and receiver is normalized to 1m. The transmit power is exponentially distributed.

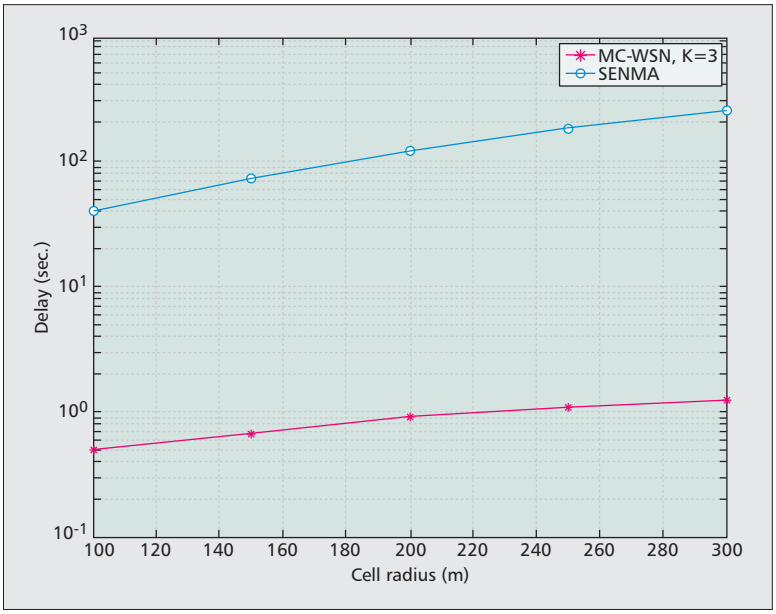

Figure 5. Delay vs. cell radius for MC-WSN and SENMA networks. Here, $n = 2000$, average per-hop distance is 10 m, departure rate from each queue is 100 packets/sec, arrival rate to a queue $\lambda_q = 0.9\vartheta$, maximum buffer size $B = 20$ packets, the packet size $b = 8$ bytes, the maximum transmission rate $c = 6.4$ kb/s, and average back-off time $\xi = 3b/c$.

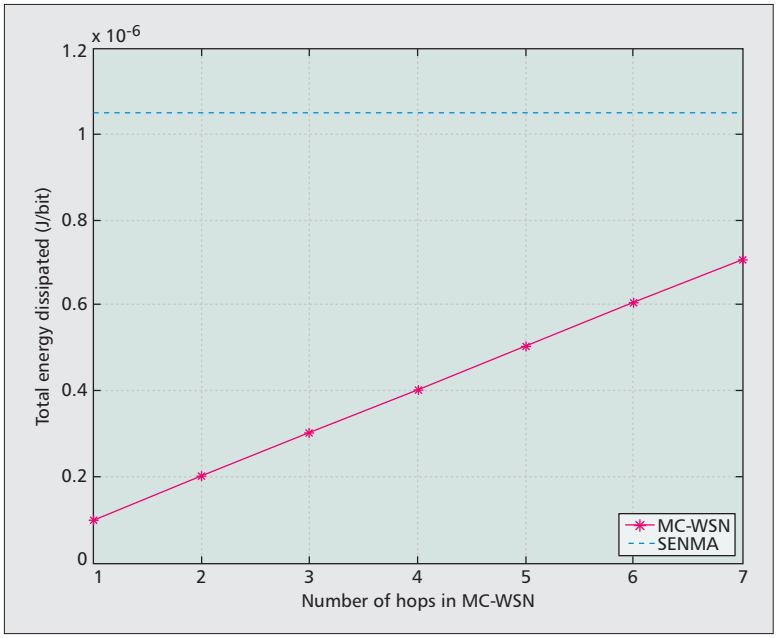

Figure 6. The energy dissipation (J/bit) vs. the number hops in N-hop MCWSN, and comparison with the single hop SENMA network. Here, we set d_{cell} = 100m, per-hop distance and the MA coverage radius is 10m, path loss exponent $\beta = 2$, $n = 2000$, $E_{tx} = E_{rx} = 50$ (nJ/bit) and $\varepsilon = 10$ (pJ/bit/m^2).

data. To compute the delay, the sink then compares the time stamp with the actual time of reception. If the delay is greater than a certain threshold, then an exceptional behavior is detected. In this case, more measurements can be scheduled or requested for the network to locate the specific communication failure.

Access Authentication: Accountability and Privacy Protection

Access authentication is critical in network security and serves as the base for user accountability, in which the user can be held accountable for its behavior. Comparing with the ad hoc network, the hierarchical structure in hybrid networks make it easier for authentication and tracking of user accountability.

For N-hop networks, authentication can be implemented through a centralized authentication center (AuC) in the device-level. The hybrid network structure and routing diversity also enables the N-hop network to support network-level authentication.

For the device-level authentication, the authentication service is initiated by the fixed network and can be implemented through a simple challenge-response based authentication protocol. The authentication requires a shared secret key between each device and the centralized authentication center (AuC).

When a wireless device A needs to initiate a communication with another wireless device B, A makes an initial access request to B. The access request should contain the device identity ID, the BS that A accesses and can be authenticated through the AuC. After receiving the access request, B works as a proxy and forwards A 's access request to the fixed BS and the AuC for A to be authenticated. The AuC then issues a random access *Challenge* and send it to A through the BS and B. Upon receiving the *Challenge*, A computes the response Response = E_{k_A} (*Response*) based on the *Challenge* and the secret key k_A shared between A and the AuC. The computed response will be sent back to the AuC through B and the BS for authentication. If the authentication is successful, the communication between A and B can be established. Otherwise, the access request from A will be rejected by B. This process only provides authentication of A to B. If two-way authentication is required, B can be authenticated to A following the same procedures.

For the network-level authentication, the authentication can be split into two phases: the end-user device authentication to network access point (NAP) (such as BS, CH etc.) and the authentication between the NAPs through a mutually trusted network server in the hierarchical structure such as the AuC. The end-user device authentication to the NAP can either be performed by the NAP locally or through the AuC. In both scenarios, the NAP can be viewed as a proxy for the end-user device and can provide end-user privacy protection to hide the communication events between the source and the destination.

In addition to authentication and accountability services, compared with traditional centralized network, the routing diversity in hybrid networks make the transmissions more robust under unexpected network failure or hostile attacks. At the same time, the routing diversity can also be exploited to achieve better privacy protection.

Conclusions

In this article, we first revisit the evolution of wireless systems and discussed the general design criterions of wireless networks. It is observed that in order to achieve a good balance among capacity, reliability, delay, and flexibility, a network should be sufficiently structured and at the same time should provide adequate ad hoc flexibility. On the evolution of wireless networks, this is reflected as the merging of centralized and ad hoc networks, leading to the development of hybrid networks. In an effort to provide a unified framework for existing wireless systems, especially hybrid networks, we introduce the concept of N-hop networks. Under the N-hop framework, we discuss the analytical characterization of network performance in terms of throughput, delay, and energy efficiency, and also look into the security perspectives on the balance between user accountability and privacy protection. It is shown that the N-hop framework includes most of the existing systems as special cases, and provides a flexible and tractable platform for network design, management, and performance evaluation.

Acknowledgment

This research was supported in part by NSF grants CNS-0746811, CNS-0845812, CNS-1117831, CNS-1217206, ECCS-1232109.

References

[1] R. Frenkiel, "Creating Cellular: A history of the AMPS project (1971–1983) [History of Communications]," *IEEE Commun. Mag.*, vol. 48, no. 9, 2010, pp. 14–24.

[2] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," *Ad Hoc Networks*, vol. 1, no. 1, 2003, http://www.sciencedirect.com/science/article/pii/S1570870503000131, pp. 13–64.

[3] H. Wu *et al.*, "Integrated Cellular and Ad Hoc Relaying Systems: iCAR," *IEEE JSAC*, vol. 19, no. 10, 2001, pp. 2105–15.

[4] A. Zadeh *et al.*, "Self-Organizing Packet Radio Ad Hoc Networks with Overlay (Soprano)," *IEEE Commun. Mag.*, vol. 40, no. 6, 2002, pp. 149–57.

[5] G. Neonakis Aggelou and R. Tafazolli, "On the Relaying Capability of Next-Generation GSM Cellular Networks," *IEEE Personal Communi.*, vol. 8, no. 1, pp. 40–47, 2001.

[6] K. Doppler *et al.*, "Device-to-Device Communication as an Underlay to LTE-Advanced Networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[7] A. C. Guyton and J. E. Hall, *Textbook of Medical Physiology*, Philadelphia, Saunders, 2000.

[8] G. Mergen, Z. Qing, and L. Tong, "Sensor Networks with Mobile Access: Energy and Capacity Considerations," *IEEE Trans. Commun.*, vol. 54, no. 11, pp. 2033–44, Nov. 2006.

[9] M. Abdelhakim *et al.*, "Architecture Design of Mobile Access Coordinated Wireless Sensor Networks," *Int'l. Conf. Commun.*, *ICC'13*, 2013.

[10] —, "Distributed Detection in Mobile Access Wireless Sensor Networks Under Byzantine Attacks," *IEEE Trans. Parallel and Distributed Systems*, vol. 99, 2013.

[11] V. Naware, G. Mergen, and L. Tong, "Stability and Delay of Finite-User Slotted ALOPH with Multipacket Reception," *IEEE Trans. Info. Theory*, vol. 51, no. 7, Jul. 2005, pp. 2636–56.

[12] Y. Chen and J. Andrews, "An Upper Bound on Multihop Transmission Capacity with Dynamic Routing Selection," *IEEE Trans. Info. Theory*, vol. 58, no. 6, June 2012, pp. 3751–65.

[13] D. Bertsekas and R. Gallager, *Data Networks*, Prentice-Hall, 1992.

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, Oct. 2002, pp. 660–70.

Biographies

TONGTONG LI [SM] (tongli@egr.msu.edu) received the Ph.D. degree in Electrical Engineering in 2000 from Auburn University. She is an Associate Professor in the Department of Electrical and Computer Engineering at Michigan State University. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory and statistical signal processing. Dr. Li is currently serving as an Associate Editor for IEEE Trans. Signal Processing.

MAI ABDELHAKIM (abdelhak@egr.msu.edu) received her B.Sc. and M.Sc. degrees in Communications Engineering from Cairo University in 2006 and 2009, respectively. Ms. Abdelhakim is currently a graduate research assistant in the Electrical and Computer Engineering department at Michigan State University, where she expects to receive her Ph.D. degree in May 2014. Her current research focuses on reliable and efficient communications in sensor networks and high-speed wireless networks.

JIAN REN [SM] (renjian@egr.msu.edu) received the BS and MS degrees both in mathematics from Shaanxi Normal University, and received the Ph.D. degree in EE from Xidian University, China. He is an Associate Professor in the Department of ECE at Michigan State University. His current research interests include cryptography, network security, cloud computing security, energy efficient sensor network security protocol design, privacy-preserving communications, and cognitive networks. He is a recipient of the US National Science Foundation Faculty Early Career Development (CAREER) award in 2009.

Compared with traditional centralized network, the routing diversity in hybrid networks make the transmissions more robust under unexpected network failure or hostile attacks. At the same time, the routing diversity can also be exploited to achieve better privacy protection.